DMH POLICY

Title: Management of Protected Health Information	**Policy #: 07-01** **Date Issued: 08/17/07** **Effective Date: 09/17/07**
Approval by Commissioner	
Signature: Patricia Mackin	**Date:**

I. PURPOSE

The purpose of this policy is to ensure that the Department of Mental Health (DMH), a Covered Entity under the federal Health Insurance Portability and Accountability Act (Public Law 104-191), known as HIPAA, is in compliance with that Act and with the Commonwealth of Massachusetts' requirements concerning the privacy, collection, disclosure, security, integrity and availability of Protected Health Information (PHI). This includes safeguarding physical access to DMH Sites that maintain PHI either in hard copy or on DMH Electronic Information Resources. This policy repeals DMH Policy #03-2 (Management of Protected Health Information) and DMH Policy #98-6 (Security and Confidentiality Policy for DMH Computerized Information Systems Containing Client Records or Data), Commissioner's Directive #2 (Guidelines for E-mail Users), and the following DMH AIT policies and guidelines: Policy DMH-AIT-STD 99-1 (Network Security Password Policy), Policy DMH-AIT-STD 99-2 (Network System Security Policy), Policy DMH-AIT-STD 99-3 (Internal Use Policy), DMH E-mail Guidelines, and the DMH Computer User's Responsibility Handbook, dated December 14, 1998.

II. SCOPE

This policy is applicable to all DMH offices, DMH-operated facilities and programs.

III. DEFINITIONS

Administrator-in-Charge: The DMH Workforce Member with administrative responsibility for a DMH Central Office division (e.g., Deputy Commissioner for Mental Health Services), Area, Site, DMH-operated facility or program.

Electronic Protected Health Information (EPHI): PHI, as defined below, which is maintained in electronic storage media, such as computers (hard drives), magnetic tape or disks, optical disks and digital memory cards, or is transmitted by electronic media such as the internet, extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. (NOTE: certain transmissions, including of paper, via facsimile and via telephone are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.)

Health Insurance Portability and Accountability Act (HIPAA): Federal law (Public Law 104-191) that, in part, protects both an individual's right to keep and/or transfer his/her health insurance when moving from one job to another, and the privacy and security of the individual's Protected Health Information. Federal regulations (45 CFR Parts 160, 162 and 164) implement the privacy and security portions of HIPAA.

Notice of Privacy Practices: A document approved by the DMH Commissioner, or designee, that provides information to individuals who request or receive services from DMH on DMH's privacy practices relating to its use and disclosure of Protected Health Information.

Protected Health Information (PHI): Individually identifiable information relating to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for health care provided to an individual. (NOTE: EPHI, as defined above, is a subset of PHI. Consequently, the term PHI as used in this policy includes EPHI.)

IV. POLICY

A. DMH Administrative Responsibilities

DMH shall:

- Appoint a Privacy Officer with overall responsibility for the development and implementation of DMH policies and procedures relating to the use, disclosure, maintenance, and safeguarding of PHI, including a process for receiving complaints from individuals who believe their privacy rights have been violated.

- Appoint an Information Security Officer with overall responsibility for the development and implementation of DMH policies and procedures relating to the security, integrity and availability of EPHI.
- Develop and distribute a Notice of Privacy Practices.
- Develop and implement policies, procedures and forms consistent with HIPAA privacy regulations and state law for the use, disclosure, maintenance and safeguarding of PHI in the possession of DMH. DMH shall publish these policies, procedures and forms in a Privacy Handbook. Copies of the current Privacy Handbook shall be distributed as appropriate, posted on the DMH web sites, and be available for public inspection at DMH offices, facilities and programs.
- Develop and implement policies, procedures and forms consistent with HIPAA security regulations and state law for the security, integrity and availability of EPHI in the possession of DMH. DMH shall publish these policies, procedures and forms in an Information Security Handbook. Copies of the current Information Security Handbook shall be distributed as appropriate, posted on the DMH web sites, and be available for public inspection at DMH offices, facilities and programs.
- Modify the Notice of Privacy Practices, the Privacy Handbook, and/or the Information Security Handbook whenever there is a need to change DMH's privacy or security practices and ensure required distribution, and notification of such changes.
- Ensure that appropriate DMH employee volunteers, trainees and contracted vendors are trained on the DMH Privacy Handbook and the DMH Information Security Handbook.

B. Resolving Conflicts with Existing Policies, Procedures and Forms

This Policy, the Privacy Handbook, the Information Security Handbook and any revisions of these documents supersede any existing policies, procedures or forms that are related to the privacy and/or security of PHI, including EPHI, and are inconsistent with them.

V. POLICY IMPLEMENTATION

It is the responsibility of the DMH Commissioner, Privacy Officer and Information Security Officer, to ensure that this policy is implemented.

It is the responsibility of the DMH Privacy Officer to ensure that the Privacy Handbook and Notice of Privacy Practices are updated, as necessary, to reflect changes in laws, regulations, policies or procedures, and that training is carried out, as required.

It is the responsibility of the DMH Information Security Officer to ensure that the Information Security Handbook is updated, as necessary, to reflect changes in laws, regulations, policies or procedures, and that training is carried out, as required.

It is the responsibility of every DMH Administrator-in-Charge to ensure that the Privacy Handbook and Information Security Handbook is properly implemented at his/her office, Area, Site or DMH-operated facility or program.

VI. REVIEW OF THIS POLICY

This policy and its implementation shall be reviewed at least every three years, but immediately upon any change to federal or state law or regulation regarding the privacy and/or security of PHI and/or EPHI.