DMH POLICY

Title: Management of Protected Health Information	**Policy #: 07-01** **Date Issued:** August 17, 2007 **Effective Date:** September 17, 2007
Approval by Commissioner:  **Signature: Brooke Doyle, M.Ed., LMHC**	**Last Review/Revised:** September 23, 2025

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), is in compliance with that Act, HIPAA and Part 2, each as defined below, and with the Commonwealth of Massachusetts' requirements concerning the privacy, collection, disclosure, security, integrity and availability of Protected Health Information and Patient Identifying Information. 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 Locations.

III. DEFINITIONS

Application: A computer program designed to help people perform a certain type of work. Depending on the work for which it was designed, an application can manipulate

text, numbers, graphics, or a combination of these elements.

Electronic Protected Health Information (EPHI): Protected Health Information that is transmitted by electronic media or maintained in electronic media. (See Protected Health Information.). (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 their health insurance when moving from one job to another, and the privacy and security of the individual's Protected Health Information. For purposes of this policy, HIPAA shall include the Health Information Technology for Economic and Clinical Health Act of 2009 that strengthened the privacy and security provisions of HIPAA and any other federal laws that are implemented through the HIPAA implementing regulations at 45 CFR Parts 160, 162, and 164.

Location: A place of business operated by DMH (e.g., DMH office, division, Area, Site, Central Office, Facility, Program, office at a DMH operated group living environment or other office).

Notice(s) 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 and, as applicable, Patient Identifying Information.

Patient Identifying Information (PII): The name, address, social security number, fingerprints, photograph, or similar information by which the identity of a patient of a 42 CFR Part 2 "Program" can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information. The term does not include a number assigned to a patient of the Program, for internal use only by the Program, if that number does not consist of or contain numbers (such as a social security, or driver's license number) which could be used to identify a patient of the Program with reasonable accuracy and speed from sources external to the Program.

Part 2: Federal law (42 USC 290dd-2) that protects the confidentiality of substance use disorder information created, disclosed or used by the DMH Recovery from Addictions Program and its implementing Confidentiality of Substance Use Disorder Patient Records regulations (42 CFR Part 2).

Person in Charge: The Workforce Member having day-to-day responsibility for the management and operation of a DMH Location.

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.)

Workforce Members: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DMH, is under the direct control of DMH, regardless of whether they are paid by the DMH office, facility or program.

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 and PII, 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 applicable Notices of Privacy Practices.
- Develop and implement policies, procedures and forms consistent with HIPAA privacy regulations, Part 2, 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/or Applications, and be available to all Workforce Members.
- Develop and implement policies, procedures and forms consistent with HIPAA security regulations, Part 2, 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/or Applications, and be available to all Workforce Members.
- Modify the Notices 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 Workforce Members 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 and PII, 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 Notices 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 Person in Charge to ensure that the Privacy Handbook and Information Security Handbook is properly implemented at their Location.

VI. REVIEW OF THIS POLICY

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