DMH INFORMATION SECURITY HANDBOOK

INTRODUCTION

As a health care provider, the Department of Mental Health (DMH) is a covered entity and must implement security policies and procedures that comply with the Health Insurance Portability and Accountability Act (HIPAA), including but not limited to the Privacy and Security Rules. DMH is also an agency of the Commonwealth of Massachusetts and subject to state technology, privacy, and information security laws, regulations, rules, policies, and procedures.

DMH Policy #07-01, Management of Protected Health Information, was issued to establish the overall structure of DMH's compliance with the HIPAA and applicable state privacy and information security laws.

DMH receives a substantial amount of its Information Resources and related services, including, without limitation, hardware, software, services, personnel, contracts and infrastructure, from the Executive Office of Technology Services and Security (EOTSS) and/or the Executive Office of Health and Human Services (EOHHS) pursuant to M.G.L. c. 6A, s. 7A, M.G.L. c. 7D, and Executive Order 532.[1] In addition to DMH Policy #07-01, DMH follows and complies with various Information Resources related policies and procedures adopted by EOTSS and/or EOHHS.

This DMH Information Security Handbook (this "Handbook") sets forth the policies and procedures DMH has adopted to protect the privacy, integrity, availability, and security of Protected Health Information (PHI) that is created, received, used or maintained by DMH. This Handbook also sets forth the policies and procedures DMH has adopted to prevent, detect, contain, and correct security violations. Use of the words *must* and *should* means that something is required under this Handbook.

This Handbook is drafted consistent with and in compliance with the HIPAA and state technology, privacy, and information security laws, regulations, rules, policies, and procedures, and DMH Policy #07-01. Throughout this Handbook there are references to EOTSS and EOHHS policies and procedures applicable to and adopted by DMH.

All DMH employees, business associates, volunteers, trainees, and other persons whose use of PHI is under the direct control of DMH, must follow the procedures set forth and/or referenced in this Handbook. This Handbook is intended to be consistent with and used in tandem with the DMH Privacy Handbook.

Any questions regarding HIPAA, state information security laws, DMH Policy #07-01 or this Handbook should be directed to the DMH Information Security Officer who can be reached by e-mail at DMHSecurityOfficer@mass.gov or by phone at 617-626-8187.

[1] In furtherance of these laws and the order, DMH has, directly or indirectly, entered agreements with EOTSS and EOHHS, which include business associate terms and conditions.

Unless otherwise noted, capitalized terms used in this Handbook are defined in the Glossary.

References to chapters and sections of chapters re to this Handbook, unless otherwise stated.