CHAPTER 1
INFORMATION SECURITY MANAGEMENT STRUCTURE

I. OVERVIEW

A. Scope

Chapter 1 describes the infrastructure DMH has established to develop, implement and oversee DMH's compliance with the standards set forth in the HIPAA Security Rule. It specifies the personnel who are responsible for ensuring DMH's HIPAA security compliance in collaboration with EOTSS, EHS IT, the DMH ISO, and the DMH Privacy Officer. It also describes the following general administrative safeguards DMH has implemented as a key part of HIPAA security compliance:

- Managers and other Workforce Security Responsibilities;
- Policies and Procedures;
- Workforce Security Training; and
- Workforce Discipline.

B. HIPAA Security Standards

By complying with the HIPAA Security Rule, DMH seeks to ensure the confidentiality, integrity, and availability of all electronic information that is created, received, maintained, and/or transmitted by Workforce Members to enable DMH to provide high quality services to its clients.

Confidentiality is the assurance that electronic information is shared only among authorized persons or organizations.

Integrity is the assurance that electronic information is not changed unless an alteration is known, required, documented, validated and approved.

Availability is the assurance that systems responsible for delivering, storing and processing information are accessible when needed, by those who need them, under both routine and emergency circumstances.

II. SECURITY PERSONNEL

A. DMH Information Security Officer (DMH ISO)

The DMH ISO is appointed by the Commissioner of DMH. In collaboration with the DMH Privacy Officer, the DMH ISO is the DMH staff member responsible for ensuring that DMH is in compliance with the HIPAA

Security Rule and similar state and federal laws. The DMH ISO's responsibilities include:

1. Facilitating the development, implementation, and oversight of the activities DMH needs to undertake to be in compliance with the HIPAA Security Rule and similar federal and state laws and documenting such activities for control purposes.

2. Establishing, implementing, maintaining, and updating the DMH-wide information security policies and procedures that are required for DMH to comply with the standards set forth in the HIPAA Security Rule and similar federal and state laws. (*See* Chapter 1, Section IV.)

3. Monitoring Workforce Members' compliance with the DMH information security policies and procedures. (*See* Chapter 8, Section IV.)

4. Addressing questions, issues, and complaints about DMH's information security, reviewing Information Security Incidents, and processing security recommendations made by Workforce Members. (*See* Chapter 1, Section VII, Chapter 2, Section IV.B., and Chapter 1, Section IV.)

5. Reviewing Information Security Incidents on a DMH-wide basis for trends and to identify ways of mitigating risks. (*See* Chapter 2, Section VIII.)

6. Ensuring that regular audits are conducted with regard to Workforce Members' compliance with the DMH Information Security Handbook. (*See* Chapter 8, Section IV.)

7. Ensuring consistent application of sanctions for failure to comply with information security policies and procedures for Workforce Members and Business Associates, if applicable, in coordination and collaboration with Human Resources, management, and the DMH Legal Division, as is appropriate. (*See* Chapter 1, Section VI.)

8. Initiating, facilitating, and promoting activities to foster information security awareness within DMH. (*See* Chapter 1, Section V.)

9. Assisting in developing and monitoring the training plan that ensures all Workforce Members receive training on DMH information security policies and procedures. (*See* Chapter 1, Section V.)

10. Maintaining current knowledge of applicable federal and state security laws and accreditation standards, and monitoring advancements in information security technologies to help evaluate if any changes should be made to DMH policies or procedures relating to information security. (*See* Chapter 8, Sections II).

11. Maintaining a process and environment that allows and encourages Workforce Members to raise questions about and to report non-compliance with DMH information security policies and procedures. (*See* Chapter 1, Section VII and Chapter 2, Section III).

12. Cooperating with the federal Office for Civil Rights, other legal entities and DMH management in any compliance review or investigation regarding an alleged non-compliance by a Workforce Member of the DMH Information Security Handbook and/or with the HIPAA Security Rule.

13. Reporting on information security efforts to DMH senior management in a timely manner. (*See* Chapter 8, Section VI).

B. Information Security Coordinators

The DMH General Counsel shall designate an individual within the Central Office Legal Division to act as the Statewide Information Security Coordinator. The Statewide Information Security Coordinator reports to the DMH General Counsel, or designee.

Each Area Director and the Director of OIM shall designate an individual to act as the Information Security Coordinator for their respective Area or the OIM. On information security matters, these Information Security Coordinators report directly to the Area Director or the Director of OIM, as applicable, and indirectly to the DMH ISO.

Information Security Coordinators are responsible for assisting, the Area Directors, the Director of OIM and the DMH ISO in overseeing activities related to the security of electronic information within their respective Area or Office. The responsibilities of the Information Security Coordinators include the following:

1. Providing information, guidance, and assistance to the Area Directors, the Director of OIM and the DMH ISO in the implementation and maintenance of DMH information security policies and procedures.

2. Assisting the Area Directors, Director of OIM and the DMH ISO in monitoring Workforce Members' compliance with DMH information security policies and procedures.

3. Working with the Area Directors, Director of OIM and the DMH ISO to perform information security assessments and conducting related ongoing compliance monitoring.

4. Assisting in the Annual Review of Security Plan Compliance, including performing a walk-through of the Locations within their respective Area or DMH Facilities with the applicable Persons in Charge or designees. (*See* Chapter 6, Section II.A.4.)

5. Assisting the Area Directors, Director of OIM and the DMH ISO in reviewing Information Security Incidents, testing and updating procedures. (*See* Chapter 2, Section VIII.)

6. Providing guidance to Area or Facilities staff, as applicable, on questions relating to DMH information security policies and/or procedures.

7. Attend Information Security Coordinator Meetings as required.

C. Information Security Coordinator Meetings

The Area, OIM, and Statewide Information Security Coordinators, the DMH ISO, the DMH Privacy Officer and such other person or persons who the DMH ISO determines would benefit the Information Security Coordinator Meetings shall meet as often as the DMH ISO determines is necessary, but not less often than annually. The purpose of this group is to help the DMH ISO:

1. Ensure that DMH information security policies and procedures are being consistently interpreted and followed DMH-wide.

2. Provide a forum for discussing best practices, current federal and state information security laws, relevant accreditation standards and advancements in information security technologies that could be of use to DMH.

3. Identify Workforce Members' information security training needs.

4. Identify environmental or operational changes affecting the security of DMH's Information Resources.

5. Facilitate communication about information security issues and concerns.

III. GENERAL MANAGEMENT AND WORKFORCE RESPONSIBILITIES

A. DMH Supervisors and Managers

Although the DMH ISO is responsible for implementing and overseeing DMH activities related to compliance with the HIPAA Security Rule and similar federal and state laws, DMH Supervisors and Managers are responsible for ensuring that Workforce Members use Information Resources appropriately and in accordance with this Handbook. DMH Supervisors and Managers are to assist the DMH ISO in ensuring that:

1. Workforce Members' access to Information Resources and electronic information is limited in accordance with the DMH Privacy and DMH Information Security Handbooks and other applicable policies and procedures.

2. Workforce Members participate in security training as is required.

3. Appropriate sanctions are applied to Workforce Members who violate policies and procedures relating to information security. (*See* Chapter 1, Section VI.)

B. Workforce Members

DMH Workforce Members who, within the scope of their DMH responsibilities, create, access, transmit or receive electronic information, must comply with the provisions set forth in this Handbook and all applicable Commonwealth policies and procedures, including the Acceptable Use Policies of both EOHHS and EOTSS, while using Commonwealth issued Information Resources or, if permitted, any other electronic resource. This includes, but is not limited to:

1. Knowing how to report Information Security Incidents. (*See* Chapter 2).

2. Recognizing when their Workstation may be compromised. If a Workforce Member's Workstation exhibits any unusual behavior (e.g., rebooting itself or responding slower than normal), the Workforce Member must notify EHS Support Service.

3. Following access controls, such as password requirements.

4. Using an Information Resource only as permitted by this Handbook. (*See* Chapter 5.)

5. Attending security training as required by the Commonwealth, including by DMH. (*See* Chapter 1, Section V.)

6. Complying with Network access and use rules . (*See* Chapter 4.)

7. Cooperating with the federal Office for Civil Rights, other legal entities and DMH management regarding alleged non-compliance with this Handbook or the HIPAA Security Rule and/or the investigation of a reported Information Security Incident.

IV. POLICIES AND PROCEDURES

A. Required Policies and Procedures and their Documentation

DMH Policy #07-01 and this DMH Information Security Handbook are the policies and procedures DMH has put in place to comply with the HIPAA Security Rule. The DMH ISO is responsible for ensuring that the policies and procedures are updated and/or changed as is necessary to ensure DMH's continuing compliance with federal and state law regarding security of electronic information.

To that end, the DMH ISO ensures that the policies and procedures are reviewed in accordance with Chapter 8, Section VI. The DMH ISO also ensures that they continue to be appropriate and effective considering (1) changes that occur within DMH and (2) complaints and suggestions that are received relating to the confidentiality, integrity or availability of DMH's electronic information.

The DMH ISO is further responsible for maintaining a copy of any DMH policy and procedure, and any amendments thereto, that is promulgated for the purpose of implementing the HIPAA Security Rule or similar state or federal law, including but not limited to the DMH Policy #07-01 and this Handbook. A copy shall be retained for a minimum of six (6) years from the date the applicable policy or procedure was last in effect.

B. Workforce Members' Information Security Recommendations

Workforce Members are encouraged to make recommendations regarding changes to this Handbook. Such recommendations are to be submitted to the DMH ISO. The DMH ISO, or designee, will review the recommendations that are received and take such actions the DMH ISO, or designee, deem appropriate.

C. Additional Policies and Procedures

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). (*See* Introduction.) In addition to DMH Policy #07-01 and this Information Security Handbook, DMH follows and complies with various Information Resources related policies and procedures adopted by EOTSS and/or EOHHS.

V. TRAINING AND UPDATES

A. Workforce Information Security Training

Workforce Members are responsible for participating in the security trainings as identified in Chapter 4. The DMH ISO, in consultation with the DMH's Learning and Development Office, is responsible for facilitating and ensuring that the trainings are available, and that Workforce Members participate as specified.

1. **Training on Contingency Plans.** The Director of Emergency Management, working with the DMH ISO, shall ensure that training is developed, implemented, and periodically updated for all System Specific Business Continuity and Disaster Plans and the DMH statewide Business Continuity and Disaster Recovery Plan. (*See* Chapter 9, Section III.)

2. **Assessment of Training Needs.** The DMH ISO, in conjunction with the DMH Privacy Officer, the Information Security Coordinators and the DMH Learning and Development Office, on an ongoing basis, shall assess the need to train or retrain Workforce Members on certain DMH information security policies and procedures. The DMH ISO shall facilitate the development and implementation of trainings to meet the needs that are identified.

3. **Documentation of Training and of Participation**

   a. **Training Contents**. The content of each information security training developed and implemented by DMH must be documented and retained by the DMH ISO. The documentation shall be retained for ten (10) years from the last date of a training using the contents, or when the training no longer appears in the training record of a current Workforce Member, whichever is shorter.

b. **Attendance.** The Commonwealth's online training system (currently MassAchieve) is utilized to track Workforce Members' completion of trainings. The DMH Learning and Development Office shall keep a record of all information security trainings attended by each Workforce Member. At a minimum, such documentation shall be retained for six (6) years from the date such individual ceases to be a Workforce Member. Workforce Member training records shall be accessible to DMH Supervisors the DMH ISO and DMH Privacy Officer.

B. Updates

1. **Security Alerts for Workforce Members.** The DMH ISO, in conjuncture with the DMH Privacy Officer, shall keep Workforce Members up to date on current information regarding security issues and DMH information security policies and procedures. This shall be done through the publication of DMH Security Alerts. These Alerts shall be issued to all Workforce Members periodically to allow for effective communication. Copies of DMH Security Alerts shall be retained by the DMH ISO or DMH Privacy Officer for a minimum of six (6) years from their released date.

2. **Security Notices**. EOTSS and/or EHS IT may also send notices to Workforce Members to keep such Members abreast of Information Security Incidents and/or situations that may affect the security of information contained in Information Resources. Such notices are sent as needed. The DMH ISO, shall retain copies of such notices for a period of six (6) years from the date of issuance.

VI. SANCTIONS FOR NON-COMPLIANCE BY DMH WORKFORCE MEMBERS

DMH must have in place, apply, and document the application of appropriate sanctions against Workforce Members who fail to comply with policies and procedures relating to information security. *See* Chapter 2 of this Handbook and Chapter 16 of the DMH Privacy Handbook.

A. General

1. **Disciplinary Action.** DMH Workforce Members who violate the DMH Information Security Handbook or any other policy and procedure relating to information security will be subject to appropriate disciplinary action, up to and including termination of employment, termination of a DMH contract, or termination of any other work relationship with DMH.

a. **Employee.** When it is determined that a DMH employee has violated the DMH Information Security Handbook, appropriate progressive disciplinary procedures must be used and documented.

b. **Non-Employee DMH Workforce Members.** Whenever it is determined that a DMH Workforce Member, who is not a DMH employee, has violated the DMH Information Security Handbook, appropriate corrective action must be taken by the Workforce Member's DMH Supervisor in conjunction with the Workforce Member's non-DMH supervisor, if any. This could include terminating a DMH contract or otherwise severing the DMH working arrangement with the Workforce Member.

2. **Violation of the HIPAA Security Rule.** Violations of the DMH Information Security Handbook, or any other policy and procedure relating to information security, may constitute a criminal or civil offense under HIPAA, or other federal or state laws. Any Workforce Member who violates such law should anticipate that DMH will provide information concerning the violation to appropriate law enforcement personnel or authorities and will cooperate with any subsequent investigation or prosecution.

3. **Professional Ethics.** Violations of the DMH Information Security Handbook, or any other policy and procedure relating to information security, may constitute violations of professional ethics and be grounds for professional discipline. Any individual subject to professional ethics guidelines and/or professional discipline should anticipate that DMH may report such a violation to appropriate licensure/accreditation agencies and cooperate with any professional investigation or disciplinary proceedings.

B. Documentation

1. **DMH Employees.** If any DMH employee is sanctioned for violating this Handbook or any other policy and procedure relating to information security, the violation and the sanction imposed shall be recorded in their personnel record. Upon request, the applicable Human Resources Office shall provide the DMH ISO with a report of all sanctions relating to the violation of DMH information security policies and procedures that have been imposed since the implementation of this Handbook.

2. **Non-DMH Employees.** If any DMH volunteer, trainee, or contracted vendor or employee is sanctioned for violating this Handbook or any other policy and procedure relating to information security, the violation and the sanction imposed shall be recorded in the applicable contract

file, if any, or in a separate file created by the applicable DMH Supervisor taking the action against such a Workforce Member. The DMH Supervisor shall notify the DMH ISO immediately of all sanctions upon their being implemented and shall forward copies of all relevant documentation to the DMH ISO upon request.

VII. QUESTIONS, CONCERNS, COMPLAINTS, AND ISSUES REGARDING SECURITY ISSUES

A. Questions, Concerns, Complaints, and Issues

Questions, concerns, complaints, and issues regarding the DMH Information Security Handbook or other DMH policies and procedures relating to information security, and/or DMH's compliance with such policies and procedures, should be addressed to the DMH ISO, by one of three ways:

1. **Mail (internal or external):**
   Information Security Officer
   Department of Mental Health
   Central Office - Legal Office
   25 Staniford Street
   Boston, MA 02114

2. **E-mail:** DMHSecurityOfficer@mass.gov

3. **Telephone:** 617-626-8187

The DMH ISO must review and respond to all questions, concerns, complaints, and issues received. The disposition of each complaint documented as required in Chapter 2 of this Handbook. To the extent possible and reasonable, the DMH ISO shall inform any individual who files a complaint of how that complaint was handled.

KEY: Suspected Information Security Incidents must be reported as provided in Chapter 2, Sections III. C. and D. If for any reason a suspected Information Security Incident is reported to the DMH ISO, the DMH ISO shall refer the reporter directly to the reporting requirements in Chapter 2, if possible. If that is not possible, the DMH ISO shall report the suspected Information Security Incident in accordance with Chapter 2.

VIII. FREE FROM INTIMIDATION OR RETALIATORY ACTS

Individuals, who in good faith report violations of the DMH Information Security Handbook or any other DMH policy or procedure relating to information security; express concerns, complaints and/or issues about DMH's security policies or procedures and/or DMH’s compliance with such policies and procedures, must not be subject to intimidation, threats, coercion, discrimination, or any other retaliation or harassment as a result of reporting violations or expressing concerns, complaints, and/or issues.

Reports of possible retaliation or harassment should be directed to the DMH ISO and for employees to the applicable Human Resources Office and for clients to a Human Rights Officer.

IX. SEPARATION OF DUTIES

To the extent feasible and practical (i.e., considering available resources) in implementing this Handbook, the DMH ISO, and DMH Managers shall follow the principle of separation of duties to eliminate conflicts of interest in the responsibilities and duties assigned to individuals. Mission functions and distinct information system support functions should be divided among different roles; and support functions should be performed by different individuals. For example, if feasible and practical, personnel responsible for administering access control functions shall not also administer audit functions. Similarly, personnel developing and testing system code should not have access to production libraries. Job descriptions shall reflect the assigned duties and responsibilities that support separation of duties.

X. CITATIONS

Regulatory Reference	Security Officer 45 CFR 164.308(a)(2) Sanction Policy 45 CFR 164.308(a)(1)(ii)(C) Security Awareness and Training 45 CFR 164.308(a)(5)(i) Security Reminders and Updates 45 CFR 164.308(a)(5)(ii)(A) Policies and Procedures and Documentation Requirements 45 CFR 164.316