



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT DMH PRIVACY AND SECURITY COMPLIANCE PROGRAM	POLICY NO. 107.02	EFFECTIVE DATE 04/20/2005	PAGE 1 of 8
APPROVED BY:  Director	SUPERSEDES 500.47 04/20/2005	ORIGINAL ISSUE DATE	DISTRIBUTION LEVEL(S) 1

PURPOSE

1.1 To define the Privacy and Security Compliance Program for the Department of Mental Health (DMH).

POLICY

The Administrative requirements for the DMH's Privacy and Security Compliance Program consist of twelve sections:

- 2.1 Privacy, Security, and Confidentiality Training
- 2.2 Disciplinary Actions for Failure to Follow Applicable Privacy and Security Policies
- 2.3 Safeguards for Confidential and Protected Health Information
- 2.4 Disclosure of Protected Health information (PHI) by Whistleblowers
- 2.5 Workforce Member Crime Victims
- 2.6 Mitigation
- 2.7 Non-Retaliation
- 2.8 Waiver of Individual Rights
- 2.9 Complaints Related to Department of Mental Health Privacy and Security Practices
- 2.10 Personnel Designations
- 2.11 Implementing Changes to Privacy and Security Related Policies
- 2.12 Documentation of Privacy and Security Policies and Procedures

2.1 Privacy, Security, and Confidentiality Training

2.1.1 To ensure that members of the DMH workforce understand their roles and responsibilities in protecting patient privacy; DMH provides Privacy and Security Program training to all Workforce Members. The training provided is tailored to meet the member's need to access protected



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
DMH PRIVACY AND SECURITY COMPLIANCE PROGRAM	107.02	04/20/2005	2 of 8

information to perform assigned job duties or functions DMH shall provide:

2.1.1.1 Initial training of all current DMH Workforce Members at or near the time the privacy and security regulation becomes effective;

2.1.1.2 Training of new Workforce Members within 30 days following the member's addition to the workforce; and

2.1.1.3 Retraining of Workforce Members whose job duties are affected by a material change in policy and/or procedure.

2.1.2 Training will be documented and maintained in either electronic or hard copy format for each Workforce Member for six years.

2.2 Disciplinary Actions for Failure to Follow Applicable Privacy and Security Policies

2.2.1 DMH has policies and procedures regarding disciplinary actions that are communicated to all Workforce Members, agents, and contractors. Examples of possible sanctions or disciplinary actions include, but are not limited to: verbal warnings, notices of disciplinary action placed in personnel files, removal of system privileges, termination of employment, and sanctions or penalties imposed pursuant to contract. Workforce Members, agents, and contractors are also advised that there may be civil or criminal penalties for misuse or misappropriation of Protected Health Information (PHI) or for breach of security. Violations may result in notification to law enforcement, regulatory, accreditation, and licensure organizations.

2.2.2 If there is reason to believe a member of the workforce has failed to follow the privacy policies or security policies, or has breached patient confidentiality, then an investigation will be initiated and documented. If the allegation is substantiated through the investigation, appropriate sanctions or discipline will be applied.

2.2.3 DMH will maintain documentation related to sanctions/disciplinary actions of its workforce in either electronic or hard copy format. This



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
DMH PRIVACY AND SECURITY COMPLIANCE PROGRAM	107.02	04/20/2005	3 of 8

documentation will be retained in the Workforce Member's personnel record or other appropriate location depending on the category of the Workforce Member involved. This process will be imposed equitably throughout DMH. Sanctions or discipline will be applied commensurate with the severity, frequency, and intent of the violation or breach.

2.3 Safeguards for Confidential and Protected Health Information

2.3.1 Safeguards are the administrative, technical, and physical protective measures and controls that DMH imposes to protect the privacy and security of PHI and other confidential information.

2.3.2 These safeguards include, but are not limited to; hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices. Safeguards for Protected Health Information are described in DMH Policy 508.01, Safeguards for Protected Health Information. A full treatment of security controls for protecting all confidential electronic data is documented in the suite of security policies DMH 550.01 through 550.03, DMH 551.01 through 551.03, DMH 552.01, DMH 553.01, DMH 554.01 through 554.03, DMH 555.01 through 555.03, DMH 556.01, DMH 557.01, DMH 558.01, DMH 559.01, and 107.02.

2.3.2.1 **Administrative Safeguards:** DMH develops and maintains written policies, procedures, and technical processes that assure appropriate administrative safeguards to protect the privacy of PHI and the security of confidential information as follows:

1. Security Management Process
2. Assigned Security Responsibility
3. Workforce Security
4. Information Access Management
5. Security Awareness Training
6. Security Incident Procedures
7. Contingency Plan



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
DMH PRIVACY AND SECURITY COMPLIANCE PROGRAM	107.02	04/20/2005	4 of 8

- 8. Evaluation
- 9. Business Associate Contracts or Other Arrangements

2.3.2.2 **Physical Safeguards:** These safeguards provide reasonable protection of PHI from intentional or unintentional use. Physical Safeguards address the following policies and procedures:

- 1. Facility Access Controls
- 2. Workstation Use
- 3. Workstation Security
- 4. Device and Media Controls

2.3.2.3 **Technical Safeguards:** Technical Safeguards address the need to protect, control, and monitor access to electronic data. These safeguards include policies and procedures that address the following:

- 1. Access Control
- 2. Audit Controls
- 3. Integrity
- 4. Person or Entity Authorization
- 5. Transmission Security

2.3.3 DMH is responsible for creating, implementing, and maintaining a Risk Management Plan for both electronic and non-electronic information assets.

2.3.4 Verification of the development of safeguards is a responsibility of the DMH Privacy and Security Officers, who may consult with facility Privacy Coordinators, Security Coordinators, and/or other knowledgeable individuals.

2.4 Disclosures of Protected Health Information (PHI) by Whistleblowers

2.4.1 DMH does not violate the privacy and security regulations if a member of the DMH workforce discloses PHI to a health oversight agency, to a public health authority authorized to investigate, to a health care



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT DMH PRIVACY AND SECURITY COMPLIANCE PROGRAM	POLICY NO. 107.02	EFFECTIVE DATE 04/20/2005	PAGE 5 of 8
--	-----------------------------------	--	-----------------------------

accreditation organization, or to an attorney retained by a Workforce Member if the purpose of the disclosure is to report an allegation of unlawful conduct by DMH, a violation of professional or clinical standards, or conditions that endanger patients.

2.5 Workforce Member Crime Victims

2.5.1 DMH does not violate the privacy and security regulations if a member of its workforce who is a victim of a crime discloses PHI about the suspected perpetrator to a law enforcement official and the information disclosed is limited to the following information

- Name and address,
- Date and place of birth,
- Social Security number,
- ABO blood type and RH factor,
- Type of injury,
- Date/time of treatment,
- Date/time of death (if applicable), and
- Distinguishing physical characteristics (e.g., weight, height, gender, race, hair/eye color, facial hair, scars/tattoos)

2.6 Mitigation

2.6.1 To the extent practicable, DMH entities will mitigate any known harmful effect from the Use or Disclosure of PHI that was in violation of DMH security or privacy policies and procedures.

2.7 Non-Retaliation

2.7.1 DMH entities will not intimidate, threaten, coerce, or retaliate against persons for filing complaints; for testifying, assisting, or participating in investigations; for assisting or participating in compliance reviews; for assisting or participating in proceedings or hearings under Part C of Title XI of the Social Security Act; or for opposing rear or perceived unlawful acts or practices under this Act, provided the opposition is reasonable.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
DMH PRIVACY AND SECURITY COMPLIANCE PROGRAM	107.02	04/20/2005	6 of 8

2.8 Waiver of Individual Rights

2.8.1 DMH does not require an individual to waive his/her right to file a complaint or other rights with regard to his/her PHI as a condition for the provision of treatment or payment or employment.

2.9 Complaints Related to Department of Mental Health Privacy and Security Practices

2.9.1 DMH provides a process for filing a complaint or grievance regarding privacy practices.

2.9.2 All complaints or grievances are investigated and documented. This documentation includes outlining the facts of the complaint or grievance, the investigative procedures and outcomes, and final resolution. DMH maintains, in either electronic or written format, documentation related to the filing of a complaint by an individual. This documentation will be retained for six years from the date of its creation or the date when it last was in effect, whichever is later.

2.10 Personnel Designations

2.10.1 DMH has designated Privacy and Security Officers who are responsible for the development and implementation of the policies and procedures for the entity.

2.10.2 Each Manager/Program Head is responsible for working with the DMH Privacy and Security Officers in the implementation of the policies and procedures.

2.10.3 The Departmental Information Security Officer (DISO) is responsible for receiving complaints and is able to provide further information about security matters covered by the Notice of Privacy Practices.

2.11 Implementing Changes to Privacy and Security Related Policies

2.11.1 DMH policies and procedures concerning PHI are implemented, revised, or changed as necessary or required due to changes in the law, health



SUBJECT DMH PRIVACY AND SECURITY COMPLIANCE PROGRAM	POLICY NO. 107.02	EFFECTIVE DATE 04/20/2005	PAGE 7 of 8
--	------------------------------------	--	------------------------------

care practice, or entity situation. Policies or procedures that do not materially affect the content of DMH Policy 502.01, Notice of Privacy Practices, should not be changed unless the policy or procedural revisions are necessary to comply with the privacy regulations or the policy or procedure is documented prior to the effective date of the change. Implementing changes to security policies and procedures are described in DMH Policy 555.01, DMH Data Security Documentation Requirements Policy.

2.11.1.1 Necessary revisions or changes in policies, procedures, or the Notice of Privacy Practices (Notice) are documented and implemented in a timely manner. When applicable, affected groups receive notification of the changes.

1. Policy and procedural implementation relative to a Notice are made prior to the effective date of the Notice.
2. DMH reserves the right to make changes to the Notice needed to comply with revised State and/or Federal privacy regulations or changes in DMH privacy and security policies.
3. Changes of this type relate only to PHI received or created after the effective date of the Notice and are implemented after that effective date.

2.11.1.2 Policies and procedures will be maintained in written or electronic format and retained for six years from the date of its creation or the date when it last was in effect, whichever is later.

2.12 Documentation of Privacy and Security Policies and Procedures

2.12.1 DMH documents and maintains in a written or electronic format all policies; procedures, and communications relating to the privacy practices, for six years from the date of creation or the last date it was in effect, whichever is later. Documentation of security policies and



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT DMH PRIVACY AND SECURITY COMPLIANCE PROGRAM	POLICY NO. 107.02	EFFECTIVE DATE 04/20/2005	PAGE 8 of 8
--	------------------------------------	--	------------------------------

procedures is described in DMH Policy 555.01, DMH Data Security Documentation Requirements Policy.

- 2.12.2 The D1SO and others, as appropriate, are responsible for the development, potential review and revision of the policies and procedures, and communications for their respective area(s). The period between reviews will not exceed three years. .
- 2.12.3 All policies and procedures that affect DMH should be approved in accordance with DMH's policy and procedure approval process.

AUTHORITY

MANDATED BY Code of Federal Regulations 45, Part 160 and 164; Section 164.530 "Administrative Requirements"

Code of Federal Regulations 45, Part 160 and 164; Section 164.502 "General Rules"

DMH Policy Nos.:

- 502.01, Notice of Privacy Practice
- 508.01, Safeguards for Protected Health Information
- 553.01, DMH Privacy and Security Training Policy

REVIEW DATE

This policy shall be reviewed on or before January 2010.