



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

|   |  |   |  |
|---|--|---|--|
| <b>SUBJECT</b><br><b>SECURITY AND INTEGRITY OF<br/>MANAGEMENT INFORMATION<br/>SYSTEM DATA</b> | <b>POLICY NO.</b><br><b>1200.01</b>                    | <b>EFFECTIVE<br/>DATE</b><br><b>10/01/1989</b>      | <b>PAGE</b><br><b>1 of 3</b>                 |
| <b>APPROVED BY:</b><br><b>Original signed by:</b><br><b>ROBERTO QUIROZ</b><br><br>Director    | <b>SUPERSEDES</b><br><b>104.2</b><br><b>10/01/1989</b> | <b>ORIGINAL<br/>ISSUE DATE</b><br><b>12/01/1982</b> | <b>DISTRIBUTION<br/>LEVEL(S)</b><br><b>1</b> |

**PURPOSE**

- 1.1 To assure the confidentiality, integrity, and availability of all information entered and maintained in the Department of Mental Health (DMH) Management Information System (MIS).

**DEFINITIONS**

- 2.1 Management Information System (MIS) The MIS is the mainframe-based computer system used to collect, store, process, retrieve and disseminate information regarding clients, services, providers, and staff within the DMH treatment system.
- 2.2 Short-Doyle Act This State legislation provided funding to communities to provide mental health services, stipulating standards of treatment, cost reporting, and data collection.
- 2.3 Password A password is a code issued by the MIS Division to provider and DMH headquarters staff to allow entry of and access to information using the computer terminals.
- 2.4 Inquiry An inquiry refers to the act of accessing information (using the computer terminals) from the MIS without accompanying data entry.

**POLICY**

- 3.1 All employees, whether permanent, temporary, part-time, or any other, shall be held personally accountable for their actions or negligence in ensuring the confidentiality, integrity, and availability of DMH-MIS data.
- 3.2 All DMH policies and legal requirements pertinent to confidentiality shall be maintained and observed.



| SUBJECT   | POLICY NO.     | EFFECTIVE DATE    | PAGE          |
|---|----------------|-------------------|---------------|
| <b>SECURITY AND INTEGRITY OF MANAGEMENT INFORMATION SYSTEM DATA</b> | <b>1200.01</b> | <b>10/01/1989</b> | <b>2 of 3</b> |

- 3.3 Only personnel authorized by DMH who have signed confidentiality oaths may have access to client information or be issued passwords. The respective Deputy Director or designee, in consultation with MIS Division, determines and assigns the level of access of each staff to the MIS data file.
- 3.4 No person shall allow any other person to use his/her password to access or enter data on the MIS.
- 3.5 Inquiry requests shall be limited to necessary access to data to carry out specific assigned duties and responsibilities. A record of all inquiries shall be maintained on the MIS Inquiry Only Log.
- 3.6 Inquiry and/or release of client information must be in compliance with all relevant DMH policies, including, but not limited to, the following:
  - 3.6.1 Ownership of Records and Release of Patient Information
  - 3.6.2 Procedures for the Release of Mental Health Records and/or Information
  - 3.6.3 Twenty-four (24) Hour Care Facilities Release With Patient/Legal Representative's Authorization
  - 3.6.4 Twenty-four (24) Hour Care Facilities Release Without Patient/Legal Representative's Authorization
  - 3.6.5 Confidentiality of Clinical Records
  - 3.6.6 Patient Access to Mental Health Clinical Records
  - 3.6.7 Release of Patient Records and/or Information from Mental Health Clinical Records
- 3.7 Facility/Program Directors shall be responsible for maintaining the security of the MIS terminals and peripheral equipment located in the facility.



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

| SUBJECT   | POLICY NO.     | EFFECTIVE DATE    | PAGE          |
|---|----------------|-------------------|---------------|
| <b>SECURITY AND INTEGRITY OF MANAGEMENT INFORMATION SYSTEM DATA</b> | <b>1200.01</b> | <b>10/01/1989</b> | <b>3 of 3</b> |

- 3.8 Distribution and use of reports containing confidential client information shall follow pertinent DMH confidentiality procedures, including clear labeling of each page as “Confidential” information.
- 3.9 Facility/Program Directors shall be responsible for determining, maintaining records of, and taking appropriate action for any security violations in their facility. Such action includes notification of the Chief, MIS Division. Knowledge of a security violation must be reported immediately to one’s supervisor.
- 3.10 DMH management shall ensure that the systems and operating procedures developed and operated by and for the DMH contain internal and external controls so that there is no concentration of authority sufficient for one individual to commit undetected malicious or fraudulent acts.
- 3.11 DMH management shall cultivate and maintain a high level of employee awareness of the importance of data security. This employee awareness shall at a minimum consist of a signed acknowledgement of responsibilities under this policy and other such security policies and standards the DMH has implemented.
- 3.12 Purposeful violation of this policy may result in disciplinary action up to and including dismissal. Civil penalties may also be appropriate.

**AUTHORITY**

Welfare and Institutions Code, Section 5328  
MIS Procedures Manual

**ATTACHMENTS**

[Confidentiality Oath for Password Recipients \(DMH Directly-Operated Facilities\)](#)  
[Confidentiality Oath for Password Recipients \(DMH Contract Agencies\)](#)