State of New York OFFICE OF MENTAL HEALTH	Date Issued 12/20/84	T. L. 84-6	Section # A-250
OMH OFFICIAL POLICY MANUAL	Section Administrative		
	Directive Personal Privacy Protection Law		

A. Policy Statement

It is the policy of the Office of Mental Health to protect the privacy rights of individuals about whom it collects and maintains information. To implement this policy, OMH shall fully comply with the provisions of the Personal Privacy Protection Law (PPPL). The PPPL is designed to ensure that a process is established by which individuals may know what information is being collected about them by State agencies and how the information will be used.

This policy directive establishes standards and procedures for the development, modification and maintenance of systems of records; notification of individuals from whom information is collected; responding to requests for access to or amendment or correction of records; disclosure of records and filing of an annual report.

A Privacy Compliance Officer in the Central Office is responsible for coordinating all activities related to the PPPL. Deputy Privacy Compliance Officers in the psychiatric facilities and regional offices are responsible for coordinating activities related to the PPPL at those locations and for sending all required forms and reports to the Privacy Compliance Officer.

B. Relevant Statutes and Standards

Public Officers Law, Article 6-A
Mental Hygiene Law, Section 33.13
Title 14 NYCRR, Part 520
Title 9 NYCRR, Part 295
OMH Policy Directive 8000
OMH Policy Directive QA-615

C. Definitions

1. Committee means the Committee on Open Government in the Department of State.

2. Clinical Record means those documents prepared by OMH and contained in the Uniform Case Record pertaining to the admission, legal status, assessment, treatment planning, treatment and discharge of the patient. Incident Reports are not considered part of the clinical record.

3. Deputy Privacy Compliance Officer means the OMH employee designated by the Commissioner to ensure compliance with the PPPL, Part 520 of Title 14 NYCRR and this policy directive in a particular psychiatric facility or regional office. The Director of Facility Administrative Services at each psychiatric facility is the Deputy Privacy Compliance Officer for non-clinical records in that psychiatric facility; the Facility Director in each psychiatric facility is the Deputy Privacy Compliance Officer for Clinical records in that psychiatric facility; and the Regional Director in each region is the Deputy

Privacy Compliance Officer for records in that regional office.

4. Disclose means to reveal, release, transfer, disseminate for otherwise communicate personal information or records orally, in writing or by electronic or any other means than to the data subject.

5. Personal Information means any information concerning an individual which, because of name, number, symbol, mark or other identifier, can be used to identify that individual.

6. Privacy Compliance Officer means the Central Office employee designated to coordinate all activities required by the PPPL, Part 520 of Title 14 NYCRR and this policy directive.

7. Privacy Impact Statement means a form which must be completed and sent to the Committee whenever a new system of records is developed or an existing system is substantially modified.

8. Public Safety Agency Record means a record of the Commission of Corrections, the Temporary State Commission of Investigation, the Department of Correctional Services, the Division for Youth, the Division of Parole, the Crime Victims Board, the Division of Probation or the Division of State Police or of any agency or component thereof whose primary function is the enforcement of civil or criminal statutes if such record pertains to investigations, law enforcement, confinement of persons in correctional facilities or supervision of persons pursuant to criminal conviction or court order, and any, records maintained by the division of Criminal Justice Services pursuant to sections 837, 837-a, 837-c, 838, 839, 845, 845-a of the Executive Law.

9. Record means any item, collection or grouping of personal information about an individual which is maintained and is retrievable by use of the name or other identifier of the individual. The term "record" shall not include personal information which is not used to make any determination about the individual if it is:

   a) a telephone book or directory which is used exclusively for telephone and directory information;

   b) any card catalog, book or other resource material in any library;

   c) any compilation of information containing names and addresses only which is used exclusively for the purpose of mailing agency information;

   d) personal information required by law to be maintained and required by law to be used, only for statistical research or reporting purposes.

   e) information requested by the agency which is necessary for the agency to answer unsolicited requests by the data subject for information; or

   f) correspondence files.

10. Routine Use means any use of a record or personal information relevant to the purpose for which it was collected, and which use is necessary to the statutory duties of the agency that collected or obtained the record or personal information, or necessary for that agency to operate a program specifically authorized by law.

11. System of Records means any group of records under the actual or constructive control

of any agency pertaining to one or more individuals from which personal information is retrievable by use of the name or other identifier of an individual.

D. Body of Directive

This policy directive consists of six components:

1. Responsibilities of the Privacy Compliance Officer and Deputy Privacy Compliance Officers
2. Records Management
3. Notification
4. Requests for Access to or Amendment or Correction of a Record
5. Disclosure of Records
6. Annual Report

1. Responsibilities of the Privacy Compliance Officer and Deputy Privacy Compliance Officer

A Privacy Compliance Officer designated by the Commissioner is responsible for ensuring that all the provisions of the PPPL, Part 520 of Title 14 NYCRR and this policy directive are implemented.

The Director of Facility Administrative Services at each facility is designated as Deputy Privacy Compliance Officer for all activities related to the PPPL with the exception of those activities which pertain to clinical records. The Regional Director in each region is designated as Deputy Privacy Compliance Officer for all activities related to the PPPL in the Regional Office. The facility director in each facility is designated as Deputy Privacy Compliance Officer for activities related to clinical records.

While the Privacy Compliance Officer will have overall responsibility for coordinating activities related to the PPPL, the Deputy Privacy Compliance Officers will be responsible for ensuring that the activities required by the PPPL are carried out in each psychiatric center and regional office.

a. The Privacy Compliance Officer and the Deputy Privacy Compliance Officers are responsible for coordinating the development, modification and deletion of systems of records in each psychiatric center, regional office and Central Office; and completing Privacy Impact Statements; the Privacy Compliance Officer is responsible for sending completed Privacy Impact statements to the Committee; notifying appropriate OMH staff of Committee opinions; and developing retention schedules.

b. The Privacy Compliance Officer and Deputy Privacy Compliance Officers are responsible for ensuring that individuals from or about whom personal information is collected are provided with the required notification.

c. The Privacy Compliance Officer and Deputy Privacy Compliance officers are responsible for coordinating all activities related to requests for access to or amendment or correction of records; upon request, certifying that copies of records are true copies; ensuring that statements of disagreement are included in records and that disputed portions of the record are noted when appeals have been denied; and maintaining an accounting of requests for access to or amendment or correction of records.

d. The Privacy Compliance Officer and Deputy Privacy Compliance Officers are responsible for ensuring that the required consent forms are complete prior to disclosure of records and that an account of disclosures made under specific circumstances is maintained in the record.

e. The Privacy Compliance Officer is responsible for filing an annual report with the Committee which includes OMH determinations regarding requests for access to or amendment or correction of records.

2. Records Management

All records maintained by OMH should be accurate, complete, timely and relevant. To facilitate such record keeping practices, staff responsible for maintaining systems of records or staff who collect information about individuals for inclusion in records should, whenever practical, collect information directly from the individual to whom the information pertains. Information need not be collected directly from the individual in the case of personal information which pertains to patients; information collected for the purpose of determining violations of law; or information collected for the purpose of determining when to grant or deny a license or certification.

a) Development of New System of Records and Modification of Existing System

The Privacy Compliance Officer is responsible for maintaining a list of all OMH Systems of Records (see Appendix I) and ensuring that the Committee has current information on all systems of records maintained by OMH. When developing a new system, reference should be made to this list to determine if the proposed system represents a modification of an existing system, development of a new system, or a duplication of an existing system.

Whenever a new system of records is developed or an existing system is substantially modified, a Privacy Impact Statement must be completed and filed with the Committee (see Form 321 ADM (MH) Appendix II). In Central Office, the Privacy Compliance Officer is responsible for completing all Privacy Impact Statements and submitting them to the Committee. In the psychiatric facilities and regional offices, the Deputy Privacy Compliance Officer is responsible for completing and forwarding all completed Privacy Impact Statements to the Privacy Compliance Officer for submission to the Committee. The Committee has 30 business days to review the Privacy Impact Statement to determine whether the maintenance of the system is within the lawful authority of the agency. After completing its review, the Committee will notify OMH of its opinion. OMH may not implement the system prior to receipt of this review unless the proposed system is required by law to be implemented in less than 30 business days.

Once the Committee's review has been received, the Privacy Compliance Officer is responsible for notifying the appropriate Deputy Privacy Compliance Officer and other involved staff, of the Committee's opinion. OMH may modify the proposed system based upon the Committee's comments, however, it is under no obligation to do so. Upon receipt of the Committee's response, the system may be implemented.

b) Deletion of System of Records

It is the responsibility of the Privacy Compliance Officer to inform the

Committee, in writing, whenever a system of records is deleted. When the deleted system is unique to one facility or regional office, the Deputy Privacy Compliance Officer should inform the Privacy Compliance Officer in writing, of the name and location of the system. When the system is one that exists in more than one location, the unit responsible for maintenance of the system should inform the Privacy Compliance Officer or Deputy Privacy Compliance Officer that the system will be or has been deleted.

c) Retention of Records

The Privacy Compliance Officer is responsible for developing retention schedules for all systems of records maintained by OMH in accordance with OMH policy directive 8000 and Part 295 of Title 9 NYCRR. When transferring or destroying records in accordance with retention schedules, the Privacy Compliance Officer and the Deputy Privacy Compliance Officers, shall ensure that the confidentiality of all information contained in these records is protected.

3. Notification

To ensure that individuals know what information is being maintained about them and how the information may be used, an individual must be notified of certain facts whenever personal information is initially solicited for inclusion in a record. Notification must include the following information:

a) The name of the agency and any subdivision within the agency that is requesting the personal information and the name or title of the system of records in which the information will be maintained;

b) The title, business address and telephone number of the agency official who is responsible for the system of records;

c) The legal authority granted by law, which authorizes the collection and maintenance of the information;

d) The effects on the individual, if any, of not providing all or any part of the requested information;

e) The principal purpose or purposes for which the information is to be collected; and

f) The uses which may be made of the information.

The Uniform Case Record and Patient Resource Case File are the primary documents containing information about patients. Other systems of records containing information about patients consist primarily of information derived from the Uniform Case Record and Patient Resource Case File. Patients should therefore, be provided with notification upon admission and upon first contact with a resource agent.

The notification form entitled "Clinical Record System" should be provided to a patient upon admission (see Form 324 ADM (MH) Appendix II). A copy of the "Clinical Record System" notification form should be maintained in the Uniform Case Record. The notification form entitled "Patient Resource System" should be provided to a patient upon first contact with a resource agent (see Form 325 ADM (MH) Appendix II). When the patient's treatment team determines that the patient is unable to understand the

contents of the notification, notification may be provided at a later date to be determined by the treatment team. In the case of patients under 18 years of age, except those admitted on their own application, notification should be given to a parent or legal guardian. In the case of individuals determined by the courts to be incompetent, notification should be given to the court appointed guardian.

The Employee Personal History File is the primary document containing information about employees. All employees should be provided with notification upon hiring. The notification form entitled "Employee Record System" should be used for this purpose (see Form 326 ADM (MH) Appendix II).

Once an individual has been notified, it is not necessary to provide notification when subsequent information is collected for the same record system, provided the uses of the information are the same as those stated on the notification form. Individuals should, however, be notified upon readmission or rehiring.

Notification is not required when information is collected for the purpose of determining whether administrative or criminal action should be taken for violations of law; or to make determinations to grant, or deny a license or certification.

4. Access to or Amendment or Correction of Records

Each State agency is required to promulgate regulations and develop procedures for reviewing a request from an individual for access to or amendment or correction of a record containing personal information about him or her; for making a determination on such requests; and for establishing an appeal process within the agency of an initial adverse agency determination. The OMH regulations on these subjects are contained in Part 520 of Title 14 NYCRR. While OMH is not required to grant access to or amendment or correction of certain records, such as clinical records, all individuals have the right to request access to or amendment or correction of any record maintained about them, and appeal an initial adverse agency determination to Counsel's Office.

a. Requests for Access to or Amendment or Correction of Non-Clinical Records

All requests for access to or amendment or correction of a record must be made in writing to the Privacy Compliance Officer or the appropriate Deputy Privacy Compliance Officer.

All requests must reasonably describe the record sought. The Privacy Compliance Officer or Deputy Privacy Compliance Officer is responsible for assisting the individual in identifying and requesting a record when necessary. This may include providing the individual with a description of the system of records.

The Privacy Compliance Officer or Deputy Privacy Compliance Officer must respond to all requests for access within five business days and all requests for amendment or correction within 30 days. A failure to respond to a request for access to or amendment or correction within these time frames shall be construed as a denial which may be appealed. The response shall indicate one of the following:

1) Access will be provided: The individual shall be informed whether all or part of the record will be provided, when the record will be provided, the hours for review, the copying costs, and the proof of identification which

must be provided at the time of review; or

2) The request for Access has been denied: The individual shall be informed of the reasons for denial, the right to file an appeal, and the process for filing an appeal; or

3) Request for access has been received: The individual shall be informed that the request has been received and that a decision regarding access will be made within 30 days; or

4) The amendment or correction will be made in whole or in part and will upon request, be provided to any person or governmental unit to which the record has been or will be disclosed pursuant to Section D.(5d) of this policy directive; or

5) The request for amendment or correction has been denied, the reasons for such denial, the right to appeal the decision and the process for filing an appeal.

The prepared form letter should be used to respond to all requests for access to or amendment or correction of the record (see Form 323 ADM (MH) Appendix II).

Following a decision to grant access to a record, the Privacy Compliance Officer or Deputy Privacy Compliance Officer shall ensure that the record is reviewed and that any statements or references which would violate the privacy rights of others are removed prior to granting access to the record.

A staff member must be present during a review of the record. The review must take place in an environment which provides privacy. Upon request, OMH must permit a person of the individual's choosing to be present during the review of the record or while the individual is obtaining the record.

b. Request for Access to or Amendment of Correction of Clinical Records

The PPPL does not require OMH to provide access to clinical records. It is the policy (QA-615) of OMH that patients and former patients may request access to their records and a determination to grant or deny access will be made after weighing the potential detrimental effect that access may have on the patient or others against the patients need or desire to know the contents of the record.

All requests for access to or amendment or correction of clinical records by a patient or former patient must be made to the Deputy Privacy Compliance Officer for Clinical Records (facility director) or the regional director who is the deputy privacy compliance officer for all record systems maintained in the Regional Office. If a request is made to the Privacy Compliance Officer or Deputy Privacy Compliance Officer for non-clinical records, they shall send it to the appropriate Deputy Privacy Compliance Officer for Clinical records.

The Deputy Privacy Compliance Officer must respond to all requests for access within five business days and all requests for amendment or correction within 30 days. A failure to respond within these time frames shall be construed as a denial which may be appealed. The response should indicate one of the following:

1) Access will be provided: The individual shall be informed whether all or part of the record will be provided, where the record will be provided, the hours for review, and the proof of identification which must be provided at the time of the review; or

2) The request for access has been denied: The individual shall be informed of the reasons for denial, the right to file an appeal and the process for filing an appeal; or

3) Request for access has been received: The individual shall be informed that the request has been received and that a decision regarding access will be made within 30 days; or

4) The amendment or correction will be made in whole or in part and will upon request, be provided to any person or governmental unit to which the record has been or will be disclosed pursuant to Section D.(5d) of this policy directive.

5) The request for amendment or correction has been denied, the reasons for such denial, the right to appeal the decision and the process for filing an appeal.

A request for access to or amendment or correction of a clinical record, should be reviewed according to the procedure described in OMH Policy Directive QA-615. Because of the time necessary to comprehensively review the record prior to determining whether to grant or deny access, it is expected that the most frequent response to a request for access to a clinical record, will be the response described in (3) above.

The prepared form letter should be used to respond to all requests for access to or amendment or correction of the clinical record (see Form 323 ADM (MH) Appendix II).

Following a decision to grant access to a clinical record, the Deputy Privacy Compliance Officer shall ensure that the record is reviewed and that any statements or references which would violate the privacy rights of others are removed prior to granting access to the record.

A designated staff member must be present during the review of the clinical record. The review must take place in an environment which provides privacy. (See OMH policy directive QA-615 Section (d)(3)) Upon request, OMH must permit a person of the individuals choosing to be present during the review of the record or while the individual is obtaining the record.

c. Records To Which Access May Be Denied

In addition to clinical records, OMH is not required to provide access to the following categories of records:

a) Personal information to which the individual is specifically prohibited by statute from gaining access;

b) An attorney's work product or material prepared for litigation before judicial, quasi-judicial or administrative tribunals; and

c) Public safety agency records.

Whenever a request for access to these records is received, the Privacy Compliance Officer or Deputy Privacy Compliance Officer should indicate that the request has been denied and indicate the reason for the denial.

d. Appeals

Any person who has been denied access to or amendment or correction of a record may, within 30 days of the denial, file an appeal. All appeals must be directed to Counsel's Office. Within 7 business days of receipt of an appeal concerning a request for access, or within 30 business days of receipt of an appeal concerning a request for amendment or correction, the person determining the appeal shall:

1) Provide access to or correct or amend the record; or

2) Explain in writing the reasons for further denial and inform the individual of their right to file a statement of disagreement and to seek judicial review pursuant to Article 78 of the Civil Practice Law and Rules.

e. Statement of Disagreement

When a statement of disagreement is filed, the Privacy Compliance Officer or Deputy Privacy Compliance Officer shall ensure that all disputed portions of the record are clearly noted; and that the statement of disagreement is attached as a permanent part of the record.

When providing the individual's statement of disagreement in conjunction with a disclosure made pursuant to Section D.(5d) of this policy directive, OMH may include a statement of its reasons for denying the amendment or correction.

f. Accounting of Requests for Access to or Amendment or Correction of Records

The Privacy Compliance Officer and Deputy Privacy Compliance Officers are responsible for maintaining an accounting of:

1) The number of determinations made to grant in whole, access to or amendment or correction of records including the name of the record system;

2) The number of determinations made to grant in part, requests for access to or amendment or correction of records including the name of the record system and the reason for partial granting of the record.

3) The number of determinations made to deny in whole, requests for access to or amendment or correction of records including the name of the record system and the reason for denial.

The Deputy Privacy Compliance Officers are responsible for sending a copy of this accounting (see Form 327 ADM (MH) appendix II) to the Privacy Compliance Officer at his request.

5. Disclosure

a) Records Prohibited From Disclosure

Under the PPPL, the following records are not required to be disclosed except as permitted or required by law:

1) patient records may be disclosed only as allowed in Section 33.13 of the Mental Hygiene Law or other law;

2) public safety agency records; and

3) attorney's work product or material prepared for litigation before judicial, quasi-judicial or administrative tribunals.

b) Disclosures Not Requiring a Written Request or Voluntary Consent

Records may be disclosed without a written request by or voluntary consent of the data subject under the following circumstances:

1) To officers, employees and those who contract with OMH when disclosure of the record is necessary for the performance of their duties pursuant to the purpose of the agencies;

2) Pursuant to the Freedom of Information Law, unless disclosure would constitute an unwarranted invasion of personal privacy;

3) To officers or employees of another governmental unit if the information disclosed is necessary for the receiving unit to operate a program specifically authorized by law;

4) For a routine use as defined in Section C. 8 of this policy directive;

5) When specifically authorized by statute or federal regulation;

6) To the Bureau of Census for planning or carrying out a census survey;

7) To an individual who has provided OMH with advance written assurance that the record will be used solely for the purpose of statistical research and reporting, and that the name of the data subject will not be revealed;

8) Upon showing of compelling circumstances affecting the health or safety of the individual, and provided that notification is sent to the individual at this or her last address;

9) To a public archival facility as a record with sufficient historical or other value to warrant its continued preservation;

10) Pursuant to a court ordered subpoena or other compulsory legal process;

11) For inclusion in a public safety agency record or to any governmental unit which performs as one of its' duties any activity pertaining to the enforcement of criminal law;

12) Pursuant to a search warrant;

13) To employees of another governmental unit if the record is necessary for the receiving agency to comply with an executive order, and if the record is to be used only for statistical research, evaluation or reporting and not used in making any determination about the individual.

c) Written Requests or Voluntary Consents for Disclosures

No information may be disclosed for reasons other than those listed in section (b) above, unless there is a written request or voluntary consent signed by the individual stating the following information:

1) the personal information which is to be disclosed;

2) the person or entity to which the information is to be disclosed; and

3) the uses which will be made of the personal information by the person or entity receiving it.

d) Accounting for Disclosures

The PPPL requires that an accounting be maintained in the record for all disclosures made under the following circumstances:

1. To another governmental unit when the information is necessary for the receiving unit to operate a program authorized by law and the information requested is not relevant to the purpose for which it was collected;

2. Under compelling circumstances affecting the health or safety of the individual, if upon disclosure, notification is transmitted to the individual at his or her last known address;

3. For inclusion in a public safety record or to any other governmental unit which performs as a principal function any activity pertaining to enforcement of criminal law, provided that such record is reasonably described and is requested solely for a law enforcement purpose.

The accounting must include the title of the record, date of the disclosure, nature and purpose of the disclosure and name and address of person or governmental unit to whom the record was disclosed. The "Accounting of Disclosure" form (see Form 322 ADM (MH) Appendix II) must be maintained in the record accessible to the individual for the retention period of the record or a minimum of five years, whichever is greater.

6. Annual Report

OMH must file an annual report with the Committee on or before September 1 of each year. The Privacy Compliance Officer is responsible for compiling the required information maintained by Central Office, the various facilities and regional offices and sending the report to the Committee. The Deputy Privacy Compliance Officers shall send a copy of the Access, Amendment or Correction Activity Report (see Form 327 ADM (MH) appendix II) to the Privacy Compliance Officer at his request. The annual report shall include the following information:

a) The number of determinations made to grant in whole, access to or amendment or correction of records;

b) The number of determinations to grant in part, access to or amendment or correction of records;

c) The number of determinations made to deny in whole access to, amendment or correction of records.