



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT DATA SECURITY AND INTEGRITY OF THE INTEGRATED SYSTEM	POLICY NO. 302.18	EFFECTIVE DATE 11/01/04	PAGE 1 of 6
APPROVED BY: <div style="text-align: right;">Director</div>	SUPERSEDES	ORIGINAL ISSUE DATE	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To ensure the confidentiality, integrity, and availability of all information entered and maintained in the Los Angeles County Department of Mental Health (DMH) Integrated System (IS).
- 1.2 To outline the acceptable use of the DMH Integrated System.
- 1.3 To state the requirements for formulating credentials used in the Integrated System in a manner that will not compromise the security of DMH internal databases and applications.

SCOPE

- 2.1 This policy applies to all software and applications comprising the Integrated System.
- 2.2 This policy applies to all personnel who have or are responsible for an account requiring a password in the Integrated System.

INTRODUCTION

- 3.1 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates significant changes in the level and regulatory environment governing the provision of health benefits, the delivery of and payment for healthcare services, and the security and confidentiality of individually identifiable protected health information (PHI) in written, electronic, and oral formats.

DEFINITIONS

- 4.1 Authorization The granting of the right to access PHI. Required by HIPAA for use and disclosure for reasons other than for treatment, payment, or operations.
- 4.2 Authentication The process by which a user is identified as who he/she claims to be. A measure used to verify the eligibility of a user to access PHI that is designed to protect against the fraudulent use of a system or the unauthorized transmission of information.
- 4.3 Availability The state of being usable and readily accessible.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: DATA SECURITY AND INTEGRITY OF THE INTEGRATED SYSTEM	POLICY NO. 302.18	EFFECTIVE DATE 11/01/04	PAGE 2 of 6
--	-----------------------------------	--	------------------------

- 4.4 Chief Information Office Bureau A Division of DMH that manages computerized information systems.
- 4.5 Client The person who is the subject of PHI.
- 4.6 Confidentiality The state in which PHI is shared or released in a controlled manner is not made available or disclosed to unauthorized individuals, entities, or processes. Data or information that is regarded as sensitive for some reason and must, therefore, be protected against theft or improper use and must be disseminated only to individuals or organization authorized to have it. That authorization may be granted by the client whose information is to be disclosed.
- 4.7 Confidentiality Oath A form (Attachment I) that documents the agreement of the signer to protect the PHI of clients.
- 4.8 Covered Entity All health care providers, health plans, and clearinghouses, or any entities that contain components engaged in activities that transmit PHI electronically.
- 4.9 Credentials The combination of (1) information that identifies an individual to a computer system (e.g., user ID) and (2) information known only to the individual (e.g., a password) which allows access to a computer system.
- 4.10 Disclosure The release, transfer, provision, or divulging of, or access to PHI, outside the entity holding the information. Requires a specific authorization under HIPAA unless disclosure is related to the provision of health care, Payment, or operations of the entity responsible for the PHI, or under a limited set of other circumstances, e.g., for public health reasons.
- 4.11 Electronic Information Any information that is created on a computer, transported across a data network, and stored on electronic media.
- 4.12 Entitlement The level of privilege to access protected information that has been authenticated and authorized. The level of access to PHI granted to an individual.
- 4.13 Health Care Operations Any activity of a covered entity protected by HIPAA Regulations including peer review, quality assessment, case management, training, and auditing services, fraud investigations, business planning, etc.
- 4.14 Health Information Any information, whether oral or recorded in any form or medium, that:



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: DATA SECURITY AND INTEGRITY OF THE INTEGRATED SYSTEM	POLICY NO. 302.18	EFFECTIVE DATE 11/01/04	PAGE 3 of 6
--	-----------------------------------	--	------------------------

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse;
2. Is related to the past, present, or future physical or mental health or condition of any individual;
3. Documents the provision of health care to an individual; or
4. Describes the past, present, or future payment for the provision of health care to an individual.

- 4.15 HIPAA Health Insurance Portability and Accountability Act of 1996.
- 4.16 Individually Identifiable Any information, including demographic information, collected from a Health Information individual that is created or received by a provider, plan, or clearinghouse, that (1) relates to the past, present, or future physical or mental health condition of an individual; to the provision of health care to an individual; or to the past, present, or future payment for same and (2) identifies the individual or could be reasonably used to do that.
- 4.17 Inquiry The act of accessing information from the DMH Integrated System.
- 4.18 Integrated System The multi-user production computer system used to collect, store, process, retrieve, and disseminate information regarding clients, services, providers, and staff within the DMH treatment system.
- 4.19 Integrity As related to data, the quality of being complete, unimpaired, sound, and in perfect condition.
- 4.20 Local Plan State legislation that provided funding to local government to provide mental health services, stipulating standards of treatment, cost reporting, and data collection.
- 4.21 Logon ID and Password A logon ID is a naming convention that identifies a user. A password is a code issued by the CIO Bureau to users of the Integrated System to allow entry of and access to information through personal computers. Both the logon ID and the password are required to access the Integrated System. In order for an employee to be issued a logon ID and password, he/she must sign a Confidentiality Oath.
- 4.22 Need to Know A security principle stating that a user should have access only to that data needed to perform a particular function.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: DATA SECURITY AND INTEGRITY OF THE INTEGRATED SYSTEM	POLICY NO. 302.18	EFFECTIVE DATE 11/01/04	PAGE 4 of 6
--	-----------------------------------	--	------------------------

- 4.23 Privacy Rule The HIPAA regulations that protect the privacy of health information. A Privacy Rule violation is an improper use or disclosure of PHI as the result of an innocent mistake, neglect or a deliberate action.
- 4.24 Production Software and data that are used in the formal running of a computer application, as distinguished from that not being tested or staged.
- 4.25 Protected Health Information Any individually identifiable health information collected or created as a consequence of the provision of health care by a covered entity in any form, including verbal communication with a staff member, to a client that falls under the purview of HIPAA. It is information that:
- Is created or received by a health care provider, plan, or clearinghouse;
 - Relates to the past, present, or future physical or mental health condition of an individual, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual;
 - Identifies the individual or is reasonably believed could identify the individual; and
 - Is transmitted or maintained in any form or medium.
- 4.26 Provider Any person or entity supplying medical services and who bills for or is paid for medical services “in the normal course of business.”
- 4.27 Read Access Read access refers to the act of accessing information (using the computer) from the Integrated System without the capability of write access.
- 4.28 Role Level of authorized access to the Integrated System.
- 4.29 Unauthorized Disclosure The intentional or unintentional revealing of restricted information to individuals who do not have a “need to know” that information.
- 4.30 User With respect to individually identifiable health information, a person who engages in the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. In the context of HIPAA, an individual who utilizes PHI to carry out the business of a health care provider, plan, or clearinghouse.
- 4.31 User Account Information residing in a computer system that identifies an individual as an authorized user of that system. It is one component of a user’s credentials.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: DATA SECURITY AND INTEGRITY OF THE INTEGRATED SYSTEM	POLICY NO. 302.18	EFFECTIVE DATE 11/01/04	PAGE 5 of 6
--	-----------------------------------	--	------------------------

- 4.32 Write Access Write access refers to the act of accessing information (using the computer) from the Integrated System with the ability to create, change, and/or delete.

POLICY

- 5.1 All persons, whether permanent, temporary, part-time, volunteer, or any other, shall be held personally accountable for their actions or negligence in ensuring the confidentiality, integrity, and availability of Integrated System data.
- 5.2 All DMH policies and legal requirements pertinent to confidentiality shall be maintained and observed.
- 5.3 Only personnel authorized by DMH who have signed confidentiality oaths may be issued credentials to have access to PHI. The respective Program Manager or designee determines the level of access (role) for each employee in the Integrated System.
- 5.4 No person shall allow any other person to use his/her logon ID and password to access the Integrated System.
- 5.5 Read/write access for any individual authorized to use the Integrated System shall be limited to the data necessary to carry out his/her specific assigned duties and responsibilities.
- 5.6 Inquiry and/or release of client information must be in compliance with all relevant DMH policies.
- 5.7 Distribution and use of reports containing PHI shall follow pertinent DMH Privacy policies and procedures, including clear labeling of each page as “confidential information.”
- 5.8 Facility/Program Directors shall be responsible for determining, maintaining records of, and taking appropriate action for any security violation in regard to protected health information in the Integrated System in their facility. Such action includes notification to the DMH Security Officer and Chief Information Officer.
- 5.9 Knowledge of a security violation must be reported immediately to one’s supervisor.
- 5.10 DMH shall ensure the systems and operating procedures developed and operated by and for 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.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: DATA SECURITY AND INTEGRITY OF THE INTEGRATED SYSTEM	POLICY NO. 302.18	EFFECTIVE DATE 11/01/04	PAGE 6 of 6
--	-----------------------------------	--	------------------------

- 5.11 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 responsibility under this policy and other such security policies and procedures that DMH has implemented.
- 5.12 Purposeful violation of this policy, as determined by a Departmental investigation, may result in disciplinary action up to and including dismissal. Civil penalties may also be appropriate.

AUTHORITY

Welfare and Institutions Code, Section 5328
Health Insurance Portability and Accountability Act of 1996 – <http://www.cms.hhs.gov/hipaa>

ATTACHMENT

Attachment I Confidentiality Oath



**COUNTY OF LOS ANGELES - DEPARTMENT OF MENTAL HEALTH
CIO BUREAU/Systems & Operations**

CONFIDENTIALITY OATH

The intent of this Confidentiality Form is to ensure that all County, Contractor, Pharmacy, Non-Governmental Agency (NGA), and Fee-For-Service (FFS) Network Providers employees are aware of their responsibilities and accountability to protect the confidentiality of clients' sensitive information viewed, maintained and/or accessed by the IS/PATS/MEDS/STAR on-line systems.

Further, the Department's Medi-Cal and MEDS access policy has been established in accordance with Federal and State laws governing confidentiality.

Welfare and Institutions (W&I) Code, Section 14100.2, cites the information to be regarded confidential. This information includes applicant/beneficiary names, addresses, services provided, social and economic conditions or circumstances, agency evaluation of personal information, and medical data. (See also 22 California Code of Regulations (C.C.R.), Sections 50111 and 51009.)

The Medi-Cal Eligibility Manual, Section 2-H, titled "Confidentiality of Medi-Cal Case Records," referring to Section 14100.2, a, b, f, and h, W&I Code, provides in part that:

- “(a) All types of information, whether written or oral, concerning a person, made or kept by any public office or agency in connection with the administration of any provision of this chapter...shall be confidential, and shall not be open to examination other than for purposes directly connected with administration of the Medi-Cal program.”
- “(b) Except as provided in this section and to the extent permitted by Federal Law or regulation, all information about applicants and recipients as provided for in subdivision (a) to be safeguarded includes, but is not limited to, names and addresses, medical services provided, social and economic conditions or circumstances, agency evaluation or personal information, and medical data, including diagnosis and past history of disease or disability.”
- “(f) Requires agents of the State to abide by rules and regulations governing the custody, use and preservation of all records pertaining to administration of the Medi-Cal Program.”
- “(h) States “any person who knowingly releases or possesses confidential information concerning persons who have applied for or who have been granted any form of Medi-Cal benefits...for which State or Federal funds are made available in violation of this section is guilty of a misdemeanor.”

Please read the agreement and take due time to consider it prior to signing.

I understand County, Contractor, Pharmacy, NGA, and FFS employees are prohibited from sharing their unique Logon I.D. and password with co-worker or other agencies.

Further, I understand County, Contractor, Pharmacy, NGA, and FFS employees are prohibited from obtaining, releasing, or using confidential client information from case records or computer records for purposes not specifically related to the administration of services and authorized by the state Welfare and Institutions Code (Section 14100.2).

Further, I understand violation of confidentiality of records or of these policies which are made for protection of confidentiality, may cause:

1. A civil action under the provision of the Welfare and Institutions Code Section 5330 or of Chapter 3 (commencing with Section 4330) of Part 1 of Division 4, for the greater of the following amount:
 - 1.) Ten thousand Dollars (\$10,000)
 - 2.) Three times the amount of actual damages, if any sustained by the plaintiff.
2. Disciplinary action including **suspension or termination of employment.**

Further, I understand that the County will not provide legal protection if violations of these policies or procedures occur.

I hereby certify that I have read this form and the Department of Mental Health Policy on Security and Integrity of Management Information System Data. I have knowledge of the requirements of state and federal confidentiality laws and will comply with its provisions.

I, the undersigned, hereby agree not to divulge any information or records concerning any client/patient without proper authorization in accordance with California Welfare and Institutions Code, Section 5328, et seq.

User's Name: _____
Print Signature

Employee #: _____ Terminal ID: _____ Phone #: () _____
Pharmacy, FFS, NGA Legal Entity No. or
Provider #: _____ Provider Name: _____

Address: _____ / _____ / _____
City Zip

Service Area: _____ Date: _____

CIOB USE ONLY

Approved By: _____ Date: _____
MEDS COORDINATOR