



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT INFORMATION ACCESS MANAGEMENT	POLICY NO. 551.01	EFFECTIVE DATE 04/20/2005	PAGE 1 of 3
APPROVED BY:  Director	SUPERSEDES 500.31 04/20/2005	ORIGINAL ISSUE DATE 04/20/2005	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To create administrative controls for access to Protected Health Information and other confidential and/or sensitive information. To restrict access to those persons and external entities with a need for access is a basic tenet of security.

POLICY

- 2.1 The Los Angeles County Department of Mental Health (LACDMH) must ensure that System Managers/Owners establish procedures for access authorization, access establishment, and access modification that restrict access to only those persons with a need for access to accomplish the essential tasks of their respective job functions.
- 2.2 LACDMH must verify that a Business Associate Agreement with external entities to manage access authorization, access establishment, and access modification is in place.

2.2.1 Access Authorization

LACDMH must authorize access to information resources under their control on a "need to know basis" for carrying out the essential job functions of the Workforce Members. Workforce Members are prohibited from attempting to gain unauthorized access to confidential information. LACDMH must implement access control mechanisms for electronic systems to protect against unauthorized and inadvertent use, disclosure, modification, or destruction of resources.

LACDMH must set up authorization, establishment, and modification procedures for controlling access to information. The Department Information Security Officer must assist System Managers/Owners in



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION ACCESS MANAGEMENT	551.01	04/20/2005	2 of 3

implementing access authorization procedures and determining the appropriate technical access controls.

2.2.2 Isolating Health Care Clearinghouse Function

After exercising due diligence, LACDMH has determined that it has no health care clearinghouse as defined by the Health Insurance Portability and Accountability Act of 1996 that is a part of its larger organization.

2.2.3 Access Establishment and Modification

The LACDMH Chief Information Officer (CIO) must ensure that LACDMH documents and implements procedures for establishing LACDMH Workforce Member access to electronic information (for example, through access to a workstation, transaction, program, process, or other mechanism) that is both necessary and appropriate for the job functions of the Workforce Member.

The LACDMH CIO must ensure that LACDMH documents and implements procedures that modify a user's right of access to a workstation, transaction, program, process, or other mechanism, when such modification is necessary to align each Workforce Member's access with the Workforce Member's essential job functions.

DEFINITIONS

3.1 Protected Health Information:

Individually identifiable information:

(1) Except as provided in paragraph (2) of this definition, that is:

- (i) Transmitted by electronic media;
- (ii) Maintained in any medium; or
- (iii) Transmitted or maintained in any other form or medium.

(2) Protected Health Information excludes individually identifiable health information in:

- (i) Education records



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION ACCESS MANAGEMENT	551.01	04/20/2005	3 of 3

(ii) Employment records

- 3.2 Workforce Members: Employees, volunteers, trainees, and other persons whose conduct in the performance of work for the Department or its offices, programs, or facilities is under the direct control of the Department, office, or program, regardless of whether they are paid by the Department/County.
- 3.3 System Managers/Owners: The person who is responsible for the operation and use of a system.

PROCEDURE

- 4.1 Follow the procedures detailed in Attachment 1.

AUTHORITY

- 1. **MANDATED BY** 45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.308(a)(2)
- 2. Board of Supervisors Policies:
 - 6.100, Information Technology and Security Policy
 - 6.101, Use of County Information Technology Resources

ATTACHMENT (HYPERLINKED)

- 1. [Information Access Management Procedures](#)

REVIEW DATE

This policy shall be reviewed on or before January 2010.