



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT FACILITY ACCESS CONTROL	POLICY NO. 551.02	EFFECTIVE DATE 04/20/2005	PAGE 1 of 3
APPROVED BY:  Director	SUPERSEDES 500.35 04/20/2005	ORIGINAL ISSUE DATE 04/20/2005	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To define the process for ensuring the physical protection of Los Angeles County Department of Mental Health (LACDMH) information systems and their infrastructure.

POLICY

- 2.1 LACDMH must implement policies and procedures to limit physical access to electronic information systems - and the facility in which they are housed - while ensuring that properly authorized access is allowed. These policies and procedures must be consistent with LACDMH Policy No. 508.01, Safeguards for Protected Health Information (PHI).

- 2.2 Facility Access Control must include the following components to insure the integrity, confidentiality, and availability of data:

- 2.2.1 Contingency Operations

LACDMH must be responsible for developing, testing, implementing, and maintaining the information technology (IT) component of the LACDMH Contingency Operations Plan that provides facility access when necessary to restore information systems and/or lost data under the Disaster Recovery Plan and Emergency Mode Operation Plan in the event of an emergency [as detailed in LACDMH Policy 550.03, Information Technology Contingency Plan].

- 2.2.2 IT Facility Security Plan

LACDMH must be responsible for developing, testing, implementing, and maintaining the IT component of the Facility Security Plan to safeguard the facility and the computer information assets therein from unauthorized physical access, tampering, and theft.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
FACILITY ACCESS CONTROL	551.02	04/20/2005	2 of 3

2.2.3 Physical Access Control and Validation (Personnel and Visitors)

LACDMH must be responsible for developing, testing, implementing, and maintaining the IT component of the Facility Access Control and Validation Procedure to control and validate the access of each person (including each visitor) to the facility based on his/her role or function, and to control access to software programs for testing and revision.

2.2.4 Facility Maintenance Records

DMH must be responsible for developing, testing, implementing, and maintaining a Facility Security Maintenance Record to document repairs and modifications to the physical components of the facility that are related to security (e.g., hardware, walls, doors, locks).

DEFINITIONS

- 3.1 Safeguards: Administrative, physical, and technical actions or measures, and policies and procedures to protect Protected Health Information (PHI) and other confidential and/or sensitive information.
- 3.2 Access: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.
- 3.3 System Managers/Owners: The person who is responsible for the operation and use of a system.

For a more complete definition of terms used in this policy and/or procedure, see the LACDMH Security Glossary, Attachment 1 of Policy No. 555.02, Information and Technology Security.

PROCEDURE

Follow the procedures detailed in Attachment 1.



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
FACILITY ACCESS CONTROL	551.02	04/20/2005	3 of 3

AUTHORITY

1. **MANDATED BY 45** Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.310(a)(1) and (a)(2)(i-iv)
2. Board of Supervisors Policy 6.106, Physical Security

CROSS REFERENCE

1. DMH Policy No. 508.01, Safeguards for Protected Health Information

ATTACHMENT (HYPERLINKED)

1. [Facility Access Control Procedures](#)

REVIEW DATE

This policy shall be reviewed on or before January 2010.