



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	POLICY NO. 508.01	EFFECTIVE DATE 07/11/2016	PAGE 1 of 11
APPROVED BY: <i>Robin Kay Ph.D.</i> Acting Director	SUPERSEDES 500.21 02/15/2013	ORIGINAL ISSUE DATE 04/14/2003	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To establish safeguards that must be implemented by the Los Angeles County Department of Mental Health (LACDMH/Department) in order to protect the confidentiality of Protected Health Information (PHI).

DEFINITION

- 2.1 **Protected Health Information (PHI):** Is information that is (i) created or received by a health care provider, health plan, employer or health care clearinghouse; (ii) relates to the past, present or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present or future payment or the provision of payment of individual; and (iii) leads to a reasonable basis for believing that the information can be used to identify a particular individual.
- 2.2 **Particularly Sensitive Health Information:** PHI that is generally considered highly confidential including, but not limited to, mental health, substance abuse, genetics, and sexually transmitted disease information, including HIV/AIDS.
- 2.3 **Workforce:** Employees, volunteers, trainees and other persons whose conduct in their work is under the direct control of LACDMH, whether or not they are paid by the County.
- 2.4 **Landline Telephone:** Refers to a telephone which uses a solid telephone line such as metal wire or fiber optic cable for transmission.

POLICY

- 3.1 Set forth below are policies establishing minimum administrative and physical standards regarding the safeguarding of PHI that will be enforced by LACDMH. The Department may develop additional policies and procedures that are stricter



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	508.01	07/11/2016	2 of 11

than the parameters set forth below in order to maximize the safeguarding of PHI in support of their specific circumstances and requirements. The development and implementation of policies and procedures in addition to those stated herein must be approved by the Los Angeles County Chief HIPAA Privacy Officer.

- 3.2 LACDMH will implement appropriate administrative, technical, and physical safeguards which will protect PHI from any intentional, unintentional, or incidental use or disclosure that is in violation of the Department's Privacy Policies or the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. This requirement applies to all types of PHI in any form, i.e., oral, paper, or electronic.
- 3.3 The Department workforce must reasonably safeguard PHI to limit incidental use or disclosure made pursuant to an otherwise permitted or required use or disclosure.

PROCEDURE

4.1 Administrative Safeguards

- 4.1.1 Incidental/Oral Communications: The Department's workforce must exercise due care to avoid unnecessary disclosure of PHI through oral communications. Conversations in public areas should be avoided unless necessary to further client care, research, or teaching purposes. Voices should be modulated and attention paid to unauthorized listeners in order to avoid unnecessary disclosure of PHI. Client identifying information should be disclosed during oral conversation only when necessary to further treatment, payment, teaching, research, or operational purposes. Dictation and telephone conversations should be conducted away from public areas if possible. Speakerphones should be used only in private areas. Computer monitors, printers, fax machines, whiteboards, and any other equipment that displays PHI should be placed where passers-by cannot see them. The type of PHI found on a sign-in sheet or included when paging a client should be limited to the least amount of information necessary to accomplish the purpose.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	508.01	07/11/2016	3 of 11

- 4.1.2 Cellular Telephones: The use of cellular telephones is not prohibited as a means of using or disclosing PHI. However, their use poses a higher risk of interception as compared to landline telephones. Landline telephones should be used if the conversation will involve the disclosure of PHI. Use of cellular devices must comply with LACDMH Policy No. 1201.01, Assignment and Use of Cellular Telephones (Reference 1).
- 4.1.3 Telephone Messages: Telephone messages and appointment reminders may be left on answering machines and voice mail systems unless the client has requested an alternative means of communication pursuant to LACDMH Policy No. 501.04, Client Rights to Request Confidential Communication of Protected Health Information (Reference 2). Each provider and/or clinic should limit the amount of PHI that is disclosed in a telephone message. The content of appointment reminders should not reveal Particularly Sensitive Health Information directly or indirectly. Telephone messages regarding test results or containing information that links a client's name to a particular medical condition should be avoided.
- 4.1.4 Faxes: The following procedures must be followed when faxing PHI:
- 4.1.4.1 Only the PHI necessary to meet the requester's needs should be faxed.
 - 4.1.4.2 Particularly sensitive health information should not be transmitted by fax, except in emergency situations if required by a government agency. If Particularly Sensitive Health Information must be faxed, the recipient should be notified immediately prior to the transmission and, if possible, the sender should immediately confirm the transmission was completed.
 - 4.1.4.3 LACDMH should designate employees who can fax or approve the faxing of PHI. Unauthorized employees, students, and volunteers should never fax PHI.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	508.01	07/11/2016	4 of 11

- 4.1.4.4 Unless otherwise permitted or required by law, a properly completed and signed authorization must be obtained before releasing PHI to third parties for purposes other than treatment, payment, or health care operations as provided in LACDMH Policy No. 500.01, Use and Disclosure of Protected Health Information Requiring Authorization (Reference 3). PHI may be faxed to an individual if he/she requests access to his/her own PHI in accordance with LACDMH Policy No. 501.01, Clients' Right to Access Protected Health Information and Confidential Data (Reference 4).
 - 4.1.4.5 All faxes containing PHI must be accompanied by a cover sheet that includes a confidentiality notice. Use LACDMH Fax Cover for Transmitting PHI (Attachment 1).
 - 4.1.4.6 Reasonable efforts should be made to ensure that fax transmissions are sent to the correct destination. Frequently used numbers should be pre-programmed into fax machines or computers to avoid misdialing errors. Pre-programmed numbers should be verified on a routine basis. The numbers of new recipients should be verified prior to transmission.
 - 4.1.4.7 Fax machines must be located in secure areas not readily accessible to visitors and clients. Incoming faxes containing PHI should not be left on or near the machine.
 - 4.1.4.8 Fax confirmation sheets should be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet should be attached to the document that was faxed.
 - 4.1.4.9 All instances of misdirected faxes containing PHI should be investigated and mitigated pursuant to LACDMH Policy No. 506.01, Mitigation of Harm (Reference 5).
- 4.1.5 Mail: PHI should be mailed within the County's departments in sealed envelopes. PHI mailed outside the County should be sent via first



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	508.01	07/11/2016	5 of 11

class mail and should be concealed. Appointment reminders may be mailed to clients unless the client has requested an alternative means of communication pursuant to LACDMH Policy No. 501.04, Client Rights to Request Confidential Communication of Protected Health Information.

4.2 Physical Safeguards

4.2.1 Paper Records: Paper records containing PHI and clinical records must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of physical barrier should be used to protect paper records from unauthorized access.

4.2.1.1 Paper records and clinical records on desks, counters, or nurses' stations must be placed face down or concealed to avoid access by unauthorized persons.

4.2.1.2 Paper records should be secured when the office is unattended by persons authorized to have access to paper records.

4.2.1.3 Original paper records and clinical records should not be removed from the premises unless necessary to provide care or treatment to a client or required by law.

- LACDMH workforce members should not remove paper records or clinical records for their own convenience.
- Any paper records and clinical records removed from LACDMH premises should be checked out according to each program's written internal procedures and should be returned as quickly as possible.
- The safety and return of the medical records checked out or removed are the sole responsibility of the person who checked them out.



SUBJECT SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	POLICY NO. 508.01	EFFECTIVE DATE 07/11/2016	PAGE 6 of 11
--	------------------------------	--	-------------------------

- Paper records and clinical records that are removed from LACDMH premises must not be left unattended in places where unauthorized persons can gain access.
- Paper records and clinical records must not be left in unlocked automobiles or in view of passers-by.
- The theft or loss of any paper record or clinical record should be reported to the designated Privacy Officer so that mitigation options can be considered.

4.2.2 Destruction Standards: PHI must be discarded in a manner that protects the confidentiality of such information. Paper and other printed materials containing PHI should be destroyed or shredded. PHI or sensitive data stored on media or electronic devices (e.g., diskettes, tapes, zip disks, CDs, DVDs, USB flash drives, and other electronic storage devices) must be deleted or the device destroyed using a LACDMH approved method.

The LACDMH has contracted with a disposal vendor as a business associate to securely pick up, shred, or otherwise destroy PHI. LACDMH workforce members must contact the DMH Helpdesk and make arrangements to securely transport all media containing PHI to the DMH Chief Information Office Bureau (CIOB) headquarters. Portable storage media brought in or picked up for disposal will be destroyed by CIOB in accordance with internal media destruction procedures.

- 4.2.2.1 PHI files and documents awaiting disposal must be stored in containers that are appropriately labeled and are properly disposed of on a regular basis.
- 4.2.2.2 Storage rooms containing confidential information awaiting disposal must be locked after business hours or when authorized staff are not present.
- 4.2.2.3 Centralized bins or containers used for disposed confidential information must be sealed, clearly labeled “Confidential,” “PHI,” or some other suitable term and placed in a locked storage room.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	508.01	07/11/2016	7 of 11

4.2.2.4 Facilities or sites that do not have protected storage rooms or centralized waste/shred bins must implement reasonable procedures to minimize access to PHI.

4.2.3 Physical Access:

4.2.3.1 Persons authorized to enter areas where PHI is stored or viewed must wear identifiable LACDMH employee badges or be escorted by an authorized County employee.

4.2.3.2 Persons attempting to enter an area where PHI is processed must have prior authorizations from LACDMH management.

4.2.3.3 Employees must not allow others to use or share their badges and must verify access authorization for unknown persons entering an area where PHI is stored or processed.

4.2.4 Escorting Visitors or Clients: Visitors and clients must be appropriately monitored when on Department premises where PHI is located to ensure they do not access PHI on other clients without permission. This means that persons who are not part of the LACDMH workforce should not be in areas in which clients are being seen or treated or where PHI is stored without appropriate supervision.

4.2.5 Computer/Work Stations: Computer monitors must be positioned away from common areas or a privacy screen must be installed to prevent unauthorized access or observation. Suggested means for ensuring this protection include:

4.2.5.1 Use of polarized screens or other computer screen overlay devices that shield information on the screen.

4.2.5.2 Placement of computers out of the visual range of persons other than the authorized user.

4.2.5.3 Clearing information from the screen when the monitor is not being used.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	508.01	07/11/2016	8 of 11

4.2.5.4 Using password protected screen savers when computer workstations are not in use.

4.3 Technical Safeguards:

4.3.1 Technical safeguards regarding the protection of PHI maintained in electronic form will be developed as part of the efforts to implement security best practices and the HIPAA Security Regulations and are incorporated into this policy by reference.

4.3.2 Authorized LACDMH workforce members may email PHI or Confidential Data when it is first encrypted using the LACDMH Secure Messaging Solution. The secure transmission of that email is only available when using approved email systems such as DMH Outlook, DMH Outlook Web Access or DMH issued smart phones in accordance with LACDMH Policy No. 557.02, Appropriate Use of Email for Transmitting PHI and/or Confidential Data (Reference 6).

4.3.3 All Portable Electronic Devices (including, but not limited to, mobile devices, smart phones, smart wearables, smart watches, smart glasses, laptops, notebooks, tablets, iPads, iWatches, USB drives, external drives, cameras, audio and video recorders, and other devices capable of storing data) must be County issued and Encrypted or equipped with technical, administrative, or procedural safeguards that have been approved by the Department Information Security Officer and Department HIPAA Privacy Officer or their designees to protect the stored information from unauthorized access while at rest or transport.

4.3.4 Use of non-DMH issued or personally owned portable electronic device or use of non-DMH issued or personally owned stationary computing equipment:

4.3.4.1 All LACDMH Workforce members are prohibited from using their personal computing devices at the workplace.

4.3.4.2 Field Workforce members are prohibited from using non-DMH portable computing devices while performing LACDMH duties.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	508.01	07/11/2016	9 of 11

- 4.3.4.3 Teleworkers that have been preapproved to use their personally owned computing devices to perform LACDMH assignments are prohibited from storing sensitive or confidential information such as PHI or Personally Identifiable Information (PII) on their respective non-County issued devices.
- 4.3.4.4 All LACDMH Workforce members are prohibited from using their personal portable electronic devices (including, but not limited to, mobile devices, smart phones, smart wearables, smart watches, smart glasses, laptops, notebooks, tablets, iPads, iWatches, USB drives, external drives, cameras, audio and video recorders, other devices capable of storing data, and other devices that directly or wirelessly connect with these non-County issued devices) for any County business (including, but not limited to calls, emails, texting, voice or video messaging, and chatting) with LACDMH clients or associates.
- 4.3.4.5 Performing any of the above communicative actions with or about a LACDMH client with any person using a non-County issued portable electronic device is also prohibited.
- 4.3.4.6 Using non-County issued portable electronic device to take photographs or videos of LACDMH Clients or their property that can identify them in any way is prohibited.
- 4.3.5 The phone number of any County issued portable electronic device must remain blocked when communicating or contacting LACDMH clients and/or persons affiliated with the client. Tampering with, bypassing, or disabling the blocked cellular device's number is prohibited.
- 4.3.6 The use of County issued portable electronic devices for texting, messaging, or chatting with or about LACDMH Clients using unapproved mobile applications or the native device feature (i.e., SMS, iMessage) is strictly prohibited. Only authorized LACDMH Workforce Members who have prior approval from the LACDMH Department Information Security



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	508.01	07/11/2016	10 of 11

Officer and the LACDMH Department HIPAA Privacy Officer or their designees are permitted to text sensitive or confidential information with approved audiences by using a special mobile application that upon approval will be installed on their County issued devices.

- 4.3.7 The use of a County issued portable electronic device to take photographs or videos of LACDMH Clients or their property that can identify them in any way via unapproved mobile applications or the native device feature (i.e., SMS, iMessage) is strictly prohibited. To meet this unique business requirement, only authorized LACDMH Workforce Members that have prior approval from the LACDMH Department Information Security Officer and the LACDMH Department HIPAA Privacy Officer or their designees agree to follow specific and customized procedures and guidelines designed by the authorized officials, may be permitted to use their County issued device to take audio notes, photographs, or videos that include sensitive or confidential materials and exchange or transmit them with approved audience.

AUTHORITY

1. Code of Federal Regulations Title 45 Section 164.530(c)(1)

ATTACHMENT (Hyperlinked)

1. [LACDMH Fax Cover for Transmitting PHI](#)

REFERENCE

1. LACDMH Policy No. 1201.01, Assignment and Use of Cellular Telephones
2. LACDMH Policy No. 501.04, Client Rights to Request Confidential Communication of Protected Health Information
3. LACDMH Policy No. 500.01, Use and Disclosure of Protected Health Information Requiring Authorization
4. LACDMH Policy No. 501.01, Clients' Right to Access Protected Health Information and Confidential Data
5. LACDMH Policy No. 506.01, Mitigation of Harm



**LAC
DMH**
LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH

**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SAFEGUARDS FOR PROTECTED HEALTH INFORMATION	508.01	07/11/2016	11 of 11

6. LACDMH Policy No. 557.02, Appropriate Use of Email for Transmitting PHI and/or Confidential Data

RESPONSIBLE PARTY

LACDMH Compliance, Privacy, and Audit Services Bureau, HIPAA Privacy Office