



<b>SUBJECT</b> <b>APPROPRIATE USE OF EMAIL FOR TRANSMITTING PHI AND/OR CONFIDENTIAL DATA</b>	<b>POLICY NO.</b> <b>557.02</b>	<b>EFFECTIVE DATE</b> <b>08/15/2012</b>	<b>PAGE</b> <b>1 of 6</b>
<b>APPROVED BY:</b>  Director	<b>SUPERSEDES</b> <b>500.49</b> <b>08/15/2012</b>	<b>ORIGINAL ISSUE DATE</b> <b>08/15/2012</b>	<b>DISTRIBUTION LEVEL(S)</b> <b>1</b>

**PURPOSE**

- 1.1 To establish Los Angeles County Department of Mental Health (LACDMH; Department) workforce responsibilities for appropriate utilization of email for communicating all confidential data, including but not limited to protected health information (PHI).
- 1.2 Emailing confidential information and PHI requires maintaining the confidentiality of information and the integrity of the clinical record as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other applicable federal, State, local laws, and/or regulations as related to confidentiality.

**DEFINITIONS**

- 2.1 **Encryption:** The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission, or when it is stored on a transportable magnetic medium.
- 2.2 **Protected Health Information (PHI):** Is individually identifiable information relating 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 for health care provided to an individual.
- 2.3 **Confidential Data:** Is information that is sensitive, proprietary, or personal to which access must be restricted and whose unauthorized disclosure could be harmful to a person, process, or to an organization.
- 2.4 **LACDMH Secure Messaging System (Secure Messaging System):** An electronic solution utilized by LACDMH to encrypt email and its attachments during transmission to intended recipients.



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>APPROPRIATE USE OF EMAIL FOR TRANSMITTING PHI AND/OR CONFIDENTIAL DATA</b>	<b>557.02</b>	<b>08/15/2012</b>	<b>2 of 6</b>

- 2.5 **Workforce Member:** Employees, volunteers, trainees, and other persons whose conduct in the performance of work for LACDMH is under the direct control of the Department, regardless of whether they are paid or unpaid by the County.
- 2.6 **Authorized Workforce Member:** For the purpose of this policy a LACDMH workforce member who has completed the official training in the use of the Secure Messaging System, and has read and signed the Secure Email Agreement. (Attachment 1)

For a more complete discussion of terms used in this policy, see LACDMH Policy No. 555.02, Information and Technology Security Policy, the Information Security Glossary. (Reference 1)

**POLICY**

- 3.1 Any email to be sent that includes PHI or Confidential Data must first be encrypted through the Secure Messaging System.
- 3.2 Only authorized workforce members may send PHI or Confidential Data via email.
- 3.3 To become an “authorized workforce member” and be able to email PHI or Confidential Data, LACDMH workforce members must complete the official training in the use of the Secure Messaging System and must read and sign the Secure Email Agreement. (Attachment 1)
- 3.4 All Program Managers are responsible for maintaining the signed Secure Emailing Agreement and a list of employees in that program who are authorized to send email communication containing PHI or Confidential Data.
- 3.5 PHI and Confidential Data must only be sent from LACDMH email accounts. LACDMH workforce members, authorized or not, are strictly prohibited from sending PHI or Confidential Data from non-County email systems (e.g., Hotmail, AOL mail, Yahoo mail, G-mail, etc.)



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>APPROPRIATE USE OF EMAIL FOR TRANSMITTING PHI AND/OR CONFIDENTIAL DATA</b>	<b>557.02</b>	<b>08/15/2012</b>	<b>3 of 6</b>

- 3.6 Special pre-approval is required for transmitting the following:
  - 3.6.1 Any email containing PHI for 100 clients to 499 clients must have approval from the program manager or higher level manager.
  - 3.6.2 Any email containing PHI for 500 clients or more must have approval from the program manager AND the LACDMH Information Security Officer or designee.
- 3.7 All email to clients is considered PHI and must be sent in accordance with this Policy (See Attachment 2 for additional information regarding emailing clients).
- 3.8 All LACDMH workforce members, authorized or not, are prohibited from sending PHI and/or Confidential Data via text messages (Short Message System or SMS format).
- 3.9 LACDMH workforce members who violate this policy are subject to appropriate disciplinary action up to and including discharge.
- 3.10 LACDMH workforce members who violate this policy are subject to both civil and criminal penalties.

**PROCEDURE**

The LACDMH authorized workforce must follow the steps below when using the Secure Messaging System.

- 4.1 Authorized workforce members must verify that each intended email recipient has the “need to know” (in accordance with Section 4.4 of this policy) prior sending the email.
- 4.2 Authorized workforce members must exercise extreme care to ensure that emails containing PHI or Confidential Data are sent to the recipient’s correct email address.
- 4.3 Authorized workforce members may only use the Secure Messaging System to disclose PHI as permitted by HIPAA. The use of the Secure Messaging System



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>APPROPRIATE USE OF EMAIL FOR TRANSMITTING PHI AND/OR CONFIDENTIAL DATA</b>	<b>557.02</b>	<b>08/15/2012</b>	<b>4 of 6</b>

for PHI does not supersede the Privacy Rule related to the use and disclosure of PHI.

- 4.3.1 A valid authorization (in accordance with LACDMH Policy No. 500.01, Use and Disclosure of Protected Health Information Requiring Authorization) may be required prior to disclosing PHI using the Secure Messaging System. (Reference 3)
- 4.4 In order to protect client’s privacy and to minimize risk of unauthorized use, only the minimum necessary PHI shall be sent via email to those authorized to receive such PHI in accordance with LACDMH Policy No. 500.03, Minimum Necessary Requirements for Using and Disclosing Protected Health Information (PHI). (Reference 2)
- 4.5 Email shall only contain PHI that is factual and based on sufficient information gathered and is supported by documentation found in the clinical record. Email containing PHI is not to include opinions or determinations of psychological fitness or capacity.
- 4.6 Email communications containing PHI or Confidential Data shall not be sent to mailing distribution lists or shared email accounts (e.g., [info@organization.org](mailto:info@organization.org), [support@ABCcompany.com](mailto:support@ABCcompany.com), [inquiries@xxx.lacounty.gov](mailto:inquiries@xxx.lacounty.gov), etc.).
- 4.7 The Secure Messaging System does not encrypt the subject line of the email. Therefore, the use of PHI or Confidential Data in the ‘Subject Line’ is strictly prohibited.
- 4.8 The word “[secure]”, including brackets, must be placed at the front of the subject line on all emails containing PHI or Confidential Data in order to encrypt the email. Example: [secure] Next Appointment on May 5.
- 4.9 The use of the Secure Messaging System for transmission of PHI must be clearly documented in the clinical record per LACDMH Policy No. 401.02 by attaching relevant email communications to the clinical record and completing a progress note that references the attached documents. (Reference 4)
  - 4.9.1 Email containing PHI that is administrative in nature should be stored in administrative files and not in the clinical record.



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>APPROPRIATE USE OF EMAIL FOR TRANSMITTING PHI AND/OR CONFIDENTIAL DATA</b>	<b>557.02</b>	<b>08/15/2012</b>	<b>5 of 6</b>

- 4.9.2 Administrative files containing PHI shall be secured in the same manner as clinical documents that contain PHI. (Reference 5)
- 4.10 **All authorized workforce members must delete email containing PHI from applicable folders in the Outlook application (“Inbox”, “Sent”, “Deleted”, etc.) once the business need has been satisfied and the documentation has been completed.**
- 4.11 Texting PHI or Confidential Data is prohibited. If a text message that includes Confidential Data or PHI is sent to a LACDMH workforce member, the workforce members must respond to the sender via other means of communication (e.g., telephone or mail) with instructions to delete the text message immediately.
- 4.12 In the event that authorized workforce members become aware of wrongly sent or misdirected email containing PHI, they must follow the breach notification procedure as outlined in LACDMH Policy No. 506.03, Responding to Breach of Protected Health Information. (Reference 6)

**AUTHORITIES**

- 1. HIPAA Security Rule – 45 Code of Federal Regulations (CFR) Part 164, Subpart C, §164.312(e)(2)(ii)
- 2. Board of Supervisors Policies:
  - 6.101 Use of County Information Technology Resources
  - 6.104 Use of Electronic Mail (email) by County Employees
  - 6.105 Internet Usage Policy

**ATTACHMENTS (Hyperlinked)**

- 1. [LACDMH Secure Email Agreement](#)
- 2. [LACDMH Standards for Using Secure Email to Communicate with Clients](#)
- 3. [LACDMH Client’s Consent for Email](#)



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>APPROPRIATE USE OF EMAIL FOR TRANSMITTING PHI AND/OR CONFIDENTIAL DATA</b>	<b>557.02</b>	<b>08/15/2012</b>	<b>6 of 6</b>

**REFERENCES**

1. LACDMH Policy No. 555.02, Information and Technology Security Policy
2. LACDMH Policy No. 500.03, Minimum Necessary Requirements for Using and Disclosing Protected Health Information
3. LACDMH Policy No. 500.01, Use and Disclosure of Protected Health Information Requiring Authorization
4. LACDMH Policy No. 401.02, Clinical Records Maintenance, Organization, and Contents
5. LACDMH Policy No. 508.01, Safeguards for Protected Health Information
6. LACDMH Policy No. 506.03, Responding to Breach of Protected Health Information
7. LACDMH Policy No. 506.02, Privacy Sanctions

**RESPONSIBLE PARTY**

LACDMH - Chief Information Office Bureau