LOS ANGELES COUNTY
DEPARTMENT OF MENTAL HEALTH

Policy Title: **Appropriate Use of Email for Transmitting Protected Health Information and/or Confidential Data**
Policy Number: 557.02

PROCEDURES

Los Angeles County Department of Mental Health (DMH/Department) **authorized** workforce members must follow the steps below when using the DMH secure messaging system.

A. Authorized workforce members must verify that each intended email recipient has a "need to know" prior to sending the email. (Section F)

B. Authorized workforce members must exercise extreme care to ensure that emails containing Protected Health Information (PHI) or confidential data are sent to the recipient's correct email address.

C. When responding to an email, authorized workforce members must inspect the entire communication trail. If somewhere in its body the email contains PHI, they must send it encrypted using the DMH secure email messaging system.

D. Authorized workforce members may only use the DMH secure messaging system to disclose PHI as permitted by the HIPAA. Use of the DMH secure messaging system for PHI does not supersede the Privacy Rule related to the use and disclosure of PHI. A valid authorization may be required prior to disclosing PHI using the DMH secure messaging system. (DMH Policy 500.01)

E. In order to protect a client's privacy and minimize risk of unauthorized use, only the minimum necessary PHI shall be sent via email to those authorized to receive such PHI. (DMH Policy 500.03)

F. 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.

G. Email communications containing PHI or confidential data shall not be sent to mailing distribution lists or shared email accounts (e.g., info@organization.org, support@ABCcompany.com, inquiries@xxxx.lacounty.gov, etc.).

H. The DMH 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.

I. 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.

LOS ANGELES COUNTY
DEPARTMENT OF MENTAL HEALTH

Policy Title: **Appropriate Use of Email for Transmitting Protected Health Information and/or Confidential Data**
Policy Number: 557.02

PROCEDURES

J. The use of the DMH secure messaging system for transmission of PHI must be clearly documented in the clinical record by attaching relevant email communications to the clinical record and completing a progress note that references the attached documents. (DMH Policy 401.02)

1. Email containing PHI that is administrative in nature should be stored in administrative files and not in the clinical record.

2. Administrative files containing PHI shall be secured in the same manner as clinical documents that contain PHI. (DMH Policy 508.01)

K. **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.**

L. Texting PHI or confidential data through device's native standard SMS, EMS, MMS, IM, iMessage, and unsecure charts is prohibited. Only authorized workforce members who have been issued an approved device and are authorized by their management to have the DMH-approved secure text messaging and video chat application installed on their device, may send texts or conduct video chats including ones that may contain PHI or confidential data. If a text message that includes confidential data or PHI is sent to a DMH workforce member, via standard SMS or iMessage, the workforce member must respond to the sender via other means of communication (e.g., telephone or mail) with instructions to delete the text message immediately via the above unsafe methods.

M. In the event that an authorized workforce member becomes aware of wrongly sent or misdirected email containing PHI, they must follow the breach notification procedure. (DMH Policy 506.03)

N. To become an "authorized workforce member" able to email PHI or confidential data, DMH workforce members must complete the official training in the use of the DMH secure messaging system and must read and sign the Secure Email Agreement.