LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH
hope. recovery. wellbeing.

SECURE EMAIL AGREEMENT

Los Angeles County Department of Mental Health (DMH/Department) is providing a secure email solution for its workforce to communicate all confidential data, including but not limited to Protected Health Information (PHI), while maintaining the confidentiality of information as required by the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and other applicable federal, State, and local laws or regulations related to confidentiality.

As a member of the DMH workforce, I acknowledge and agree to be bound by all the terms, conditions, and policies of this agreement, including any future amendments. I understand that my non-compliance with any portion of this agreement may result in disciplinary action including suspension, discharge, cancellation of contracts, and possible civil and/or criminal penalties. I further understand that I must review and follow DMH Policy 557.02, Appropriate Use of Email for Transmitting Protected Health Information and/or Confidential Data, as well as DMH Policy 506.02, Privacy Sanctions, and all other HIPAA privacy and security policies.

As an authorized DMH workforce member, I agree to abide by the following:

1. I shall exercise extreme care to ensure email with PHI/confidential data is sent to the recipient’s correct email address.

2. I shall email only the minimum necessary PHI to protect the client’s privacy and to minimize risk of unauthorized use of PHI.

3. I shall email only PHI that is factual and based on sufficient information gathered and supported by documentation found in the clinical record. Email shall not include opinions or determinations of psychological fitness or capacity.

4. I shall not send email communications containing PHI/confidential data to mailing distribution lists or shared email accounts.

5. I shall not include any PHI/confidential data in the email subject line.

6. I shall not text PHI/confidential data through a mobile device’s native standard short message service (SMS), enhanced messaging service (EMS), multimedia messaging service (MMS), instant messaging (IM), and iMessage. I understand that only authorized workforce members who have been issued an approved device and were 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 I receive an SMS, EMS, and/or iMessage that includes PHI/confidential data, I shall respond to the sender via other means of communication (e.g., telephone or mail) with instructions to delete the text message immediately.

7. I shall not send PHI/confidential data by non-County email systems (e.g., Yahoo Mail, Hotmail, Gmail, AOL Mail, etc.).

8. All emails to clients are considered PHI and must be encrypted. I am aware of the standards that must be followed which permit DMH workforce members to use the secure email as a method of communication with clients for specific and limited purposes (e.g., scheduling appointments, sending reminders about appointments, and treatment instructions).

The signed copy of this agreement must be maintained in workforce member’s facility personnel folder.

SECURE EMAIL AGREEMENT

9. I shall insert the word “[secure]”, including the brackets, anywhere in the subject line on all emails containing PHI/confidential data in order to encrypt the email.

10. **I shall print the final email communication, including attachments containing PHI, from an email string (both received and sent), ensure that it is placed in the client’s clinical record in the “Correspondence” section or in a non-open PHI file, and complete a progress note that references the attached email.**

    a. **Email containing PHI that is administrative in nature shall be stored in administrative files and not in the clinical record.**

    b. **Clinical and administrative-related documents containing PHI or confidential data are subject to the same security requirements.**

11. **I shall delete all email containing PHI from “Inbox”, “Sent”, “Deleted” and any other mailbox folders once they have been printed.**

12. I shall follow the breach notification procedure as outlined in DMH Policy 506.03, Responding to Breach of Protected Health Information, in the event that an email containing PHI is wrongly sent or misdirected.

13. I shall obtain approval before sending any email containing PHI for 100 to 499 clients from a program manager or higher level manager; for any email containing PHI for 500 clients or more, I shall obtain approval from the program manager AND DMH Information Security Officer (DISO) or designee.

14. I shall comply with DMH Policy 506.02, Privacy Sanctions, and other HIPAA privacy and security policies that are accessible on the DMH internet website.

I certify that the agreement and policies listed above have been reviewed with me as of the date indicated below. I have read and understand the provisions of this agreement and have completed the required training.

Employee Name (Print) Employee Signature Date

As a DMH employee performing in a management or supervisory capacity, I acknowledge that I am responsible for ensuring that employees under my authority who are authorized to send email communications containing PHI or confidential data, sign and comply with this Secure Email Agreement.

Supervisor Name (Print) Supervisor Signature Date

Program Manager Name (Print) Program Manager Signature Date

The signed copy of this agreement must be maintained in workforce member’s facility personnel folder.