

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

Policy Category: Administrative

Distribution Level: Directly-Operated Programs

Office Responsible for Review of this Policy: Chief Information Office Bureau

I. POLICY STATEMENT

The purpose of this policy is to establish Los Angeles County Department of Mental Health (DMH/Department) workforce responsibilities for appropriate utilization of email for communicating all confidential data, including but not limited to Protected Health Information (PHI).

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 (HIPAA) of 1996 and other applicable federal, State, local laws, and/or regulations as related to confidentiality.

II. DEFINITIONS

Terms used within this policy are defined in the DMH Information Technology and Security Glossary.

III. POLICY

Any email to be sent that contains PHI or confidential data must first be encrypted through the DMH secure messaging system.

Only authorized workforce members may send PHI or confidential data via email.

All program managers are responsible for maintaining the signed Secure Email Agreement and a list of employees in that program who are authorized to send emails that contain PHI or confidential data.

PHI and confidential data must only be sent from DMH email accounts. DMH workforce members, whether authorized or not, are strictly prohibited from sending PHI or confidential data from non-County email systems (e.g., Hotmail, AOL Mail, Yahoo Mail, Gmail, etc.).

DMH workforce members, whether authorized or not, are prohibited in any case from accessing their non-County and personal emails (e.g., Google, Hotmail, and Yahoo) from a County IT resource (i.e., workstation or laptop) while connected to the County Network.

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

Regardless of who the recipients may be, all emails that contain sensitive or confidential information must be encrypted and sent through the DMH secure messaging system. This includes DMH workforce member recipients as well.

Special pre-approval is required for transmitting the following:

- Any email containing PHI for 100 to 499 clients must have approval from the program manager or higher level manager.
- Any email containing PHI for 500 clients or more must have approval from the program manager AND the DMH Information Security Officer (DISO) or designee.

All emails to clients are considered PHI and must be sent in accordance with this policy and Standards for Using Secure Email to Communicate with Clients.

All DMH workforce members, whether authorized or not, are prohibited from sending PHI and/or confidential data in text format or images through any mobile device's native short message service (SMS), enhanced messaging service (EMS), multimedia messaging service (MMS), instant messaging (IM) or iMessage, and unsecure chats.

Only authorized workforce members who have been issued an approved device and are authorized by their management to have 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.

The County prohibits the "automatic" forwarding of County emails to personal and non-County email domains. Workforce members must discontinue any automatic email forwarding or disable rules that forward emails in order to minimize risks. Occasionally, sensitive information may be included as part of incoming emails and since the system is not smart enough to differentiate between sensitive and standard contents, it will not know when to activate encryption by including the trigger key. Consequently, with "[Secure]" absent from the subject line, an email that inadvertently includes PHI or confidential information will be replied to or forwarded from an DMH mailbox without appropriate security or encryption and may be intercepted by a hacker.

DMH workforce members who violate this policy are subject to appropriate disciplinary action up to and including discharge.

DMH workforce members who violate this policy are subject to both civil and criminal penalties.

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

IV. PROCEDURES

[Click here to view procedures.](#)

V. AUTHORITIES

[Board of Supervisors Policy 6.100, Information Security Policy](#)
[Board of Supervisors Policy 6.101, Use of County Information Assets](#)
[Board of Supervisors Policy 6.104, Information Classification Policy](#)
[Board of Supervisors Policy 6.105, Information Technology Audit and Risk Assessment Policy](#)
[Board of Supervisors Policy 6.200, Information Sharing and Management Policy](#)
[Center for Medicare & Medicaid Services HIPAA Security Series 4, Security Standards: Technical Safeguards](#)
[Code of Federal Regulations Title 45 Sections 164.312\(e\)\(1\) and \(2\)](#)
[DMH Policy 506.02, Privacy Sanctions](#)
[DMH Policy 555.02, Information and Technology Security Privacy Rule](#)

VI. ATTACHMENTS

[Consent for Email \(MH 708\)](#)
[DMH Information Technology and Security Glossary](#)
[Secure Email Agreement](#)
[Standards for Using Secure Email to Communicate with Clients](#)

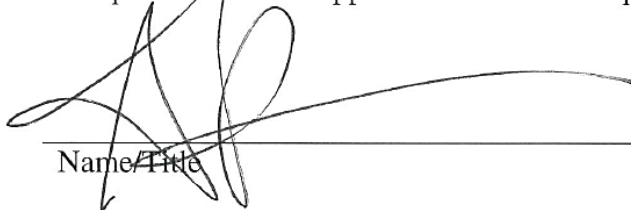
VII. EFFECTIVE DATES

This policy was effective August 15, 2012.

Review Date(s): March 27, 2019 Reviewed with Revisions

VIII. SIGNATURE, TITLE, and DATE OF APPROVAL

Required for initial approvals and all subsequent reviews and updates.



Name/Title

5-9-19

Date