CHAPTER 7
ELECTRONIC MAIL

I. OVERVIEW

Chapter 7 sets forth procedures, rules, and guidelines DMH has for the use of the Commonwealth's electronic mail (email) systems, including safeguards to protect PHI when it is sent via email.

II. GENERAL

Email is a communication tool that helps improve the day-to-day operational business of DMH. Users should exercise common sense and good judgment and use this tool appropriately. The following are DMH procedures that apply generally to the use of email on any Information Resource. These rules are in addition to the those that apply to use of electronic Information Resources set forth in Chapter 5, Section II, Use of Information Resources**,** of this Handbook.

1. Because email addresses identify the organization that sent the message (first.last@mass.gov), Users must consider email messages to be the equivalent of letters sent on official letter head. Users should ensure that all emails are written in a professional and courteous tone. Users should not write anything in an email message that they would not feel comfortable putting in a formal written document. Also in writing emails, Users should remember that emails can be stored, copied, printed and/or forwarded by recipients.

2. Users should remember that in many instances emails constitute public records and are therefore subject to public record requests under Public Record Law M.G.L. c.66 §10. Emails are also potentially discoverable in legal proceedings.

3. Emails created or received by Users are state records that may only be deleted or destroyed in accordance with the State's Statewide Records Retention Schedule.

4. Email is intended for authorized and legitimate business purposes of DMH. At any time and for any reason a DMH Manager, ACIO or designee, and/or the DMH ISO may, at their discretion, require EHS IT to restrict use of email by a User. Users have no expectation of privacy when using any Information Resources, including Commonwealth emails and email accounts.

5. The general distribution (e.g., to all Central Office) of an email containing a public service announcement or event that is sent beyond a sender's immediate work unit requires prior approval of the sender's DMH Supervisor.

Sending an email DMH-wide requires prior approval of the DMH Chief of Staff, or designee.

6. Users should be careful when addressing email messages. The TO: and CC: address lines should be confirmed to ensure that the intended recipients are included in the address lines when addressing and responding to email messages.

7. If attaching files, Users should check to make sure that the correct files have been attached.

8 Users must never send messages that are defamatory, offensive, or harassing in nature.

9. Emails should not be used to transmit unsolicited personal views on social, political, religious, or other non-business matters; email chain letters; etc. Any User receiving such an email should delete it.

10. Users should not send an email message from an email account that is not owned by the User without prior approval of the owner. If allowed, the sender shall specify that they are sending the email on behalf of the account owner.

11. Emails concealing the identity of the sender, impersonating another, or representing that the sender is someone other than the actual sender are prohibited.

12. Users may not intentionally distribute messages that contain viruses, worms or other malicious codes.

III. Email Containing PHI

A. Necessary to Perform Job Function. Users may not email PHI unless necessary to perform their job functions. Only the minimum amount of PHI necessary for the purpose should be emailed.

B. Procedures Vary Depending on Recipient.

1. To @mass.gov Addresses. PHI may be sent by email if: (a) all receivers' addresses end in "@mass.gov"; and (b) the email is sent from an address that also ends in "@mass.gov". Because state email addresses are behind the state firewall, and therefore secure, Users sending PHI to another Massachusetts state email address are not required to use the Commonwealth's Secure File and Email Delivery system.

2. **To Other Addresses.** PHI may be sent by email to an address that does not end with "@mass.gov" only through Commonwealth's Secure File and Email Delivery system (SFED).

   The following procedures must be followed to use SFED:

   i. The word **Secure:** with a colon must be placed in the subject of the email.

   ii. If a secured email is forwarded, it is no longer secure. You must delete the "FW" in the subject line and restart the secure email with the word **Secure:** with a colon in the subject line.

   Note: The SFED system has limited attachment size capacity. To send multiple or large attachments use the Commonwealth's Secure File Transfer Protocol. (*See* Chapter 5, Section IV, Electronic Transmissions.)

C. General Procedures. In using email to send PHI, the following procedures shall be followed:

1. Caution should be exercised when using the email Global Address List (GAL). When using the GAL, do not assume that a name and email address appearing in the list is a state email address (i.e., that has an @mass.gov address). Many of the names and email addresses in the list are not state employees but are actually names and email addresses that have been added to the GAL to provide a convenient way to send mail to contractors, vendors, business partners and other external entities.

2. The email must include the name of the sender, the sender's direct telephone number, and the following confidentiality notice:

   Confidentiality Notice: Protected Health Information from the Massachusetts Department of Mental Health: Protected Health Information (PHI) is personal and sensitive information related to a person's health care. If this email contains PHI, it is being emailed to you after appropriate authorization from the person or under circumstances that do not require the person's authorization.

   Important Warning: This message is intended only for the use of the person or entity to which it is addressed and may contain information that is privileged and confidential, the disclosure of which is governed by applicable law. If you are not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, the disclosure, copying or distribution of this

information is Strictly Prohibited. If you have received this message by error, please notify the sender immediately.

This requirement applies to all emails containing PHI that are sent, sent in reply or that forward the PHI to others.

3. Reasonable precautions must be taken to ensure that emails are directed to the right person and destination, (e.g., by double-checking all addressees first and last names and entity or domain addresses).

4. Discreet subject headers shall be used, such as "Secure: Personal and Confidential Communications." PHI should not be included in the subject line of an email. Client's names or initials are PHI and should not be used as the subject of an email.[1]

5. To the extent possible, emails containing PHI shall be set to require confirmation of receipt by all recipients.

D. Misdirected Emails. If a User becomes aware that they have misdirected an email containing PHI, the User should attempt to recall the email[2] and in addition should call the recipient requesting that the misdirected email and any attachments be deleted from recipient's system without reading it. If the recipient cannot be reached by telephone, another email should be sent with such instructions and asking the recipient to advise whether they read the email and/or attachment containing PHI and to confirm the deletion of the information.

If a User receives a misdirected email from another Workforce Member or a non-DMH individual or entity and the email contains PHI, the User shall attempt to contact the sender by telephone if possible or, if that is not possible, by email to notify individual/entity of the error. The misdirected email should be deleted from the unintended recipient's Inbox and then Deleted Items.

E. Accounting. An individual or their Personal or Legally Authorized Representative[3], if any, has the right to an accounting of certain types of disclosures of the individual's PHI that are made by DMH. The types of disclosures subject to this rule are limited. A User making a disclosure via email that is subject to accounting must ensure the disclosure is logged in accordance with Chapter 12, Right to an Audit Trail of Certain Disclosures of Protected Health Information, of the DMH Privacy Handbook.

---

[1] The content of Secure: emails is encrypted in transit but the subject line is not.
[2] Only emails sent to state email addresses (i.e., @mass.gov) can be recalled, if recalled before being opened by the unintended receipt. Emails sent to non-state email addresses cannot be recalled.
[3] As defined in the DMH Privacy Handbook Glossary.

IV. Remote Email Access

A. Subject to All Restrictions. A User remotely accessing email via VPN or OWA must follow all provisions of this Handbook, the DMH Privacy Handbook, and all applicable EOTSS and EOHHS policies and procedures.

B. Outlook Web Access (OWA). Users accessing email via OWA must:

1. only access OWA to perform their duties for DMH;

2. only access OWA from a DMH Workstation or other Commonwealth issued Device[4]; and

3. when in public, position the screen so as to prevent visibility by others and otherwise comply with the physical safeguards for DMH Workstations set forth in Chapter 6, Section VII, Workstations, Printers, Other Devices, and Digital Media**,** of this Handbook.

C. Access to OWA

To log on to OWA:

Go to http://www.mass.gov/ and find the "Working" tab and select "For State Employees" for the most up to date instructions for logging on to State Employee email.

V. CITATIONS

Regulatory Reference	Secure Transmissions 45 CFR 164.312(e)(1)

VI. REFERENCED POLICIES AND PROCEDURES

Statewide Records Retention Policy

VII. Related Attachment:

Email Do's and Don'ts

[4] Except in limited circumstances as permitted by the EOHHS Acceptable Use Policy.