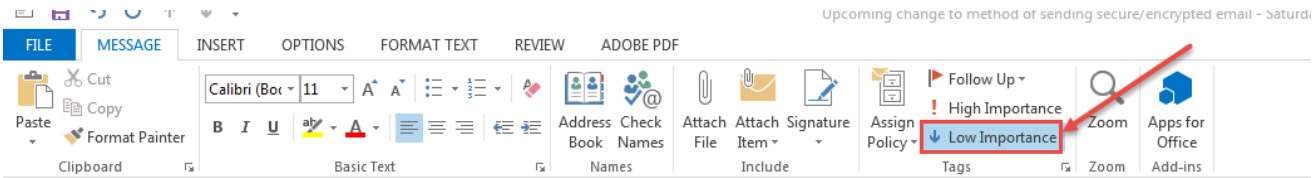
Secure/Encrypted Emails

The confidentiality of medical, psychiatric, and substance use information is protected by State and Federal statutes, rules and regulations. The statues, rules, and regulations require that we protect the client's personal health information (PHI) and personal identifiable information (PII). The law requires we obtain consent from the client/ legal representative prior to the disclosure of PHI, except under specific conditions as indicated by the laws. Confidentiality of client information must be protected at all times.

There are times when we may need to share PHI of PII information outside of the Monterey County Health Department email directory as part of the coordination and delivery of services, for these instances, the Monterey County Health Department notified all staff, regarding the procedure related to the use of encrypted emails when personal health information (PHI) and Personal Identifiable Information (PII) is sent.

Safeguards for protecting PHI and PII should be taken to minimize the risk of a potential breach in confidentiality.

- Do NOT put client name or MRN in the subject line. If absolutely necessary, please use client initials
- Double-check email addresses before you hit "reply to all" to decide if the email is required to be sent via secure email.
- Check to make sure there a no personal email addresses BEFORE you send. PHI and PII may not be sent to personal emails.
- Ensure this confidentiality statement is on your email signature: *Confidentiality Notice: This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution of this message is prohibited and may be against the law. If you are not the intended recipient, please contact the sender by replying to the original email and destroy all copies (electronic and print) of the original message.*
- To send an encrypted email, mark emails with "LOW IMPORTANCE" per information below:

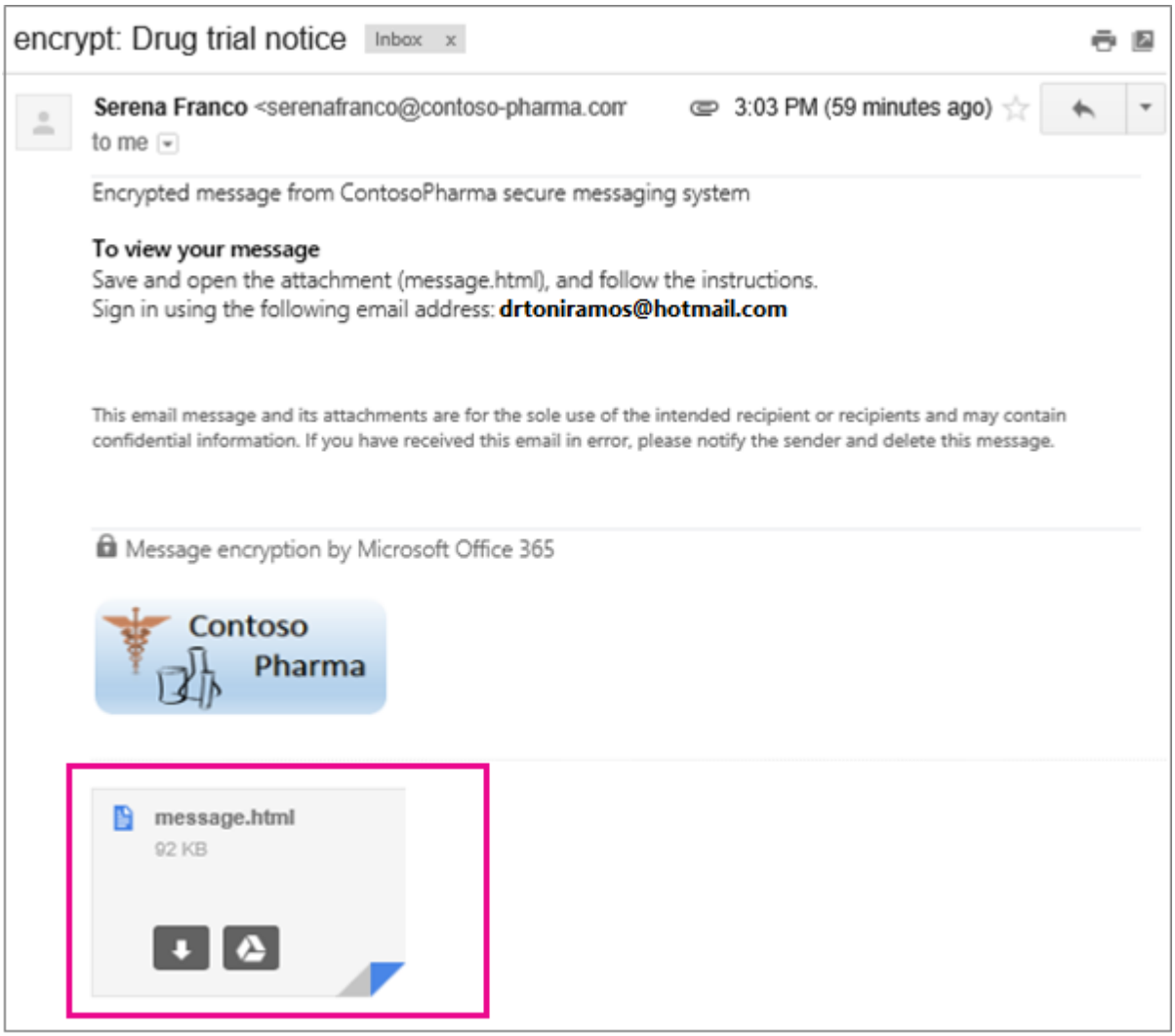


Impact to your email recipients of encrypted email message

- Recipients will have two options to open the message
    - Recipient may log in if they have a Microsoft account
    - Recipient may request a on-time passcode that will be emailed to them

What Will the Recipient of a Secure Email See?

Receive, view and reply to encrypted messages:
A message that is encrypted by Office 365 Message Encryption is delivered to a recipient's inbox just like any other email message, but it contains an HTML file attachment. After opening the attachment, the recipient can sign in or use a one-time passcode to view the message on the Office 365 Message Encryption portal. The email includes instructions for viewing the encrypted message, as in the following example (the attachment is highlighted):



Step 1: Recipient opens the HTML attachment and the following screen will appear:

Step 2: Recipient selects sign-in method and can view the contents of the encrypted message.
NOTE: If recipient is inactive for more than 15 minutes, they are automatically signed out of the encryption portal.

Step 3: Recipient can reply to an encrypted message by choosing Reply or Reply All, and then Send. An encrypted copy of the reply message is sent to the original sender.