# CentraCare Health

Message Encryption Reference Guide

Microsoft Office 365 Encryption allows users to encrypt messages as needed or automatically based on policy rules. Messages are sent seamlessly and securely.

To send an encrypted message:
- Encrypted messages can be sent from your CentraCare email account.
- Include the word **encrypt** in the subject line to send an encrypted email message on an as-needed basis.
- Policy based encryption encrypts messages based on policy rules.

  - Note: Only typed text is scanned, images and print screens are viewed as graphics. Therefore, emails containing images or print screens that include protected health information (PHI) or other confidential information must include the word **encrypt** in the subject line.

When an encrypted message is sent outside of CentraCare Health the recipient will receive an email stating that they have received an encrypted message.
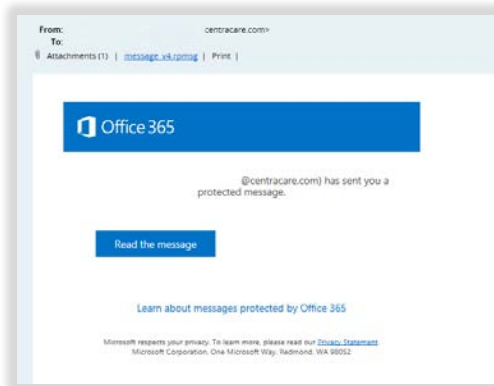

The instructions will direct them to either sign in with a Microsoft account or use a one-time passcode.
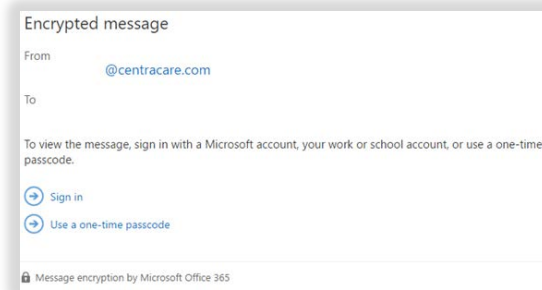
Most often the recipient will choose a one-time passcode. When this is selected, the recipient will see the following notification informing them that another email has been sent with the passcode information.
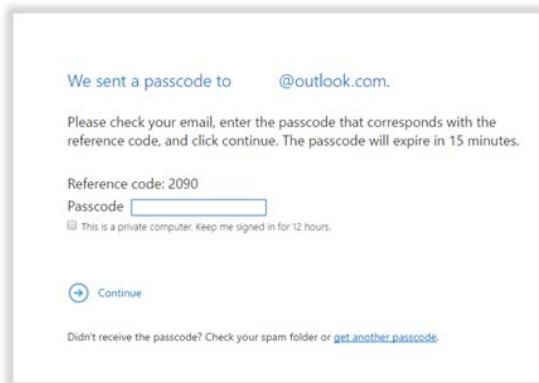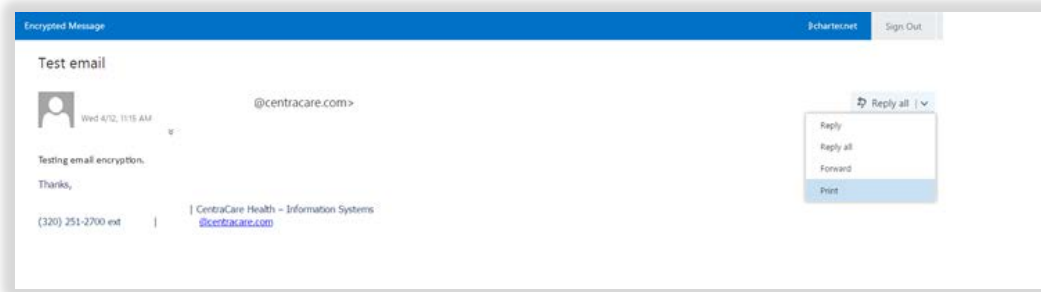

The recipient will receive an email from Microsoft Office 365 Message Encryption with the code to use to access the encrypted email.
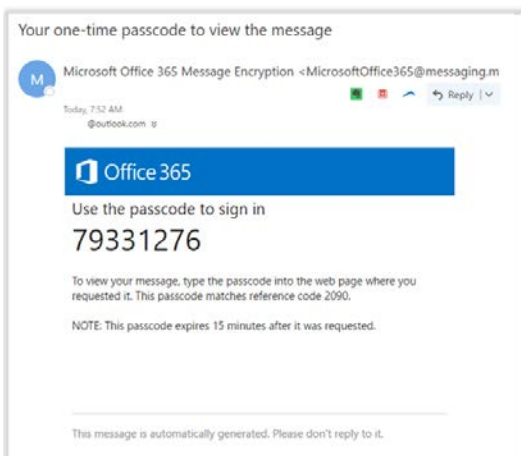
After entering the code, the encrypted email will open.
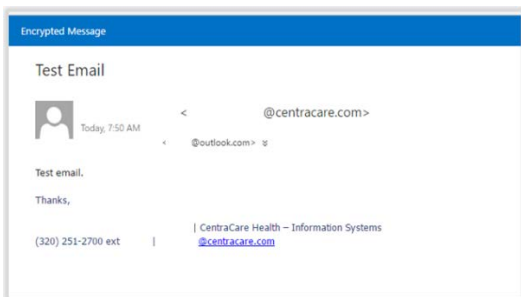
You have the ability to Reply, Reply all, Forward, and Print the Encrypted Message.

More Information:

- Email with attachments over 20 MB will need to be sent using CentraCare Health Secure Messaging and File Transfer System:

    This is Located on CentraNet > Online Tools > Email Information > Secure Email

- Emails containing payment card numbers or information (PCI) will be blocked. Please refer to CentraCare Health's policy on this topic at the following link:
    http://centranet/policies/cchs/policies/payment_card_acceptance_policy.pdf