Job Aid: Sending a Secure Message in Outlook Desktop

Trinity Health

Overview

The purpose of this job aid is to provide direction for sending secure messages to external email recipients, such as AOL, Yahoo! Mail, and Gmail recipients, outside our network through Trinity Health's Cisco IronPort Secure Email Gateway. The recipient may or may not be a Trinity Health colleague, but their personal email client is not secured on our network. When you send an email outside our network with any confidential information in it, including but not limited to PHI (Protected Health Information), PII (Personally Identifiable Information), and financial information, you must take important precautions to send it securely.

When sending secure emails to external recipients not on our network, there are procedures that both the sender and recipient must follow. Refer external recipients to this job aid for receiving and opening a secure email: Cisco Secure Email Encryption Service 6.2 Recipient Guide. If the external recipient is a non-colleague, they will not have access to the link for this job aid and you will need to share the steps and instructions with them.
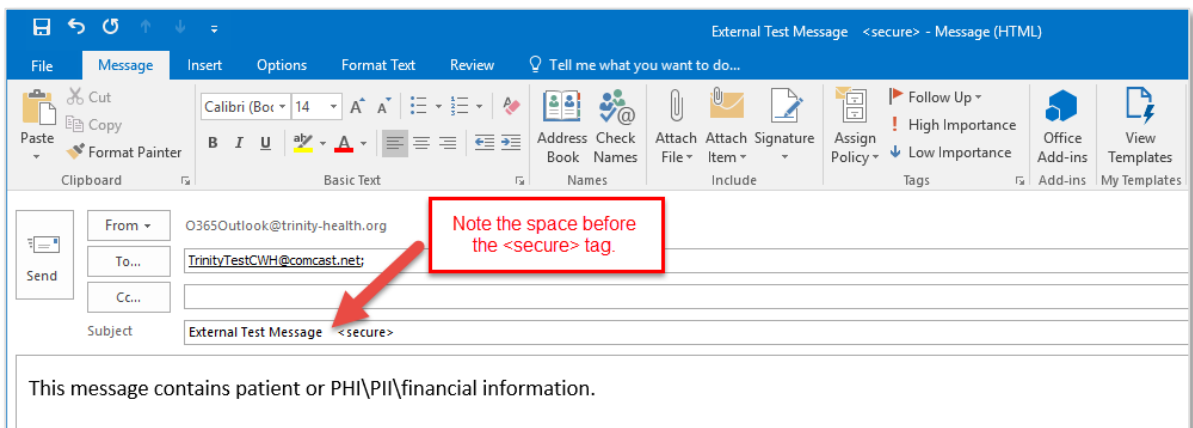
Sending a Secure Message

Inbox

1. Create a new message addressing and composing it as you normally would, and add any attachments.

2. At the beginning or end of the **Subject** line, add any one of the following tags:
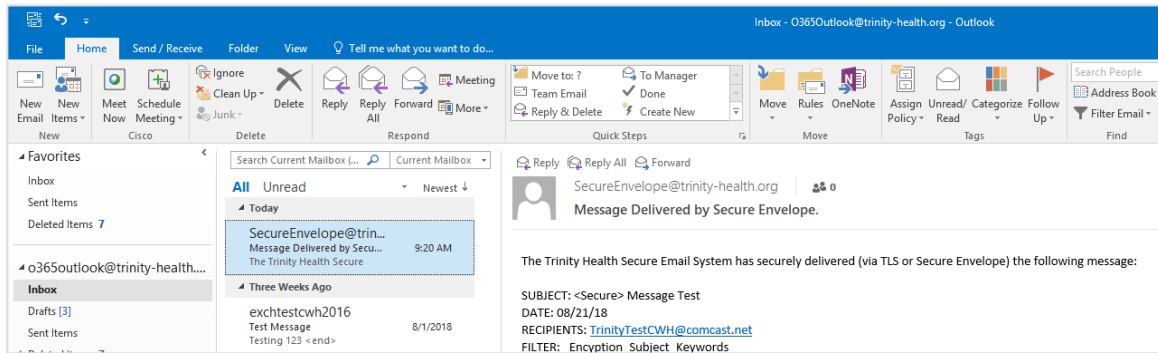
    (secure) <secure> secure

Important: There must be a space in front of or behind the secure tag. For example, a valid secure tag would be "Important messag**e <**secure>" not "Important messag**e<**secure>" with no space. Or, "Secur**e** Important message" not "Secur**e**Important message." If you don't add the space, the message will not be sent through the secure server.

Sending a Secure Message (continued)

3. Click **Send**. The message is sent securely through Trinity Health's Cisco IronPort Email Gateway to the external recipient.

   You should receive a **Message Delivered by Secure Envelope** confirmation message, stating the message was securely delivered to the recipient.

Note: The external recipient will receive an email indicating they've received a secure message. Refer external recipients to the [Cisco Secure Email Encryption Service 6.2 Recipient Guide](#) for instructions on receiving and opening a secure message.