Sending Secure Email

Encrypting e-mail protects the message from being read by anyone other than the intended recipient. UC Irvine Health has partnered with ZixCorp to provide email encryption services.

In order to protect privacy and ensure that communication between you and External representatives is secure and confidential, all of our e-mail correspondence will be encrypted.

Before you send an encrypted e-mail, be sure that:

- The information you are sending is appropriate for the recipient(s),
- The message should be encrypted, and
- Other secure delivery options are not preferable.

Note: To encrypt a message using the information below, you must send the e-mail from your UC Irvine Health's E-mail Service mailbox. If you forward or do not connect directly to UC Irvine Health E-mail Service, the options for encrypting your e-mail below will not work.

Send Encrypted E-mail

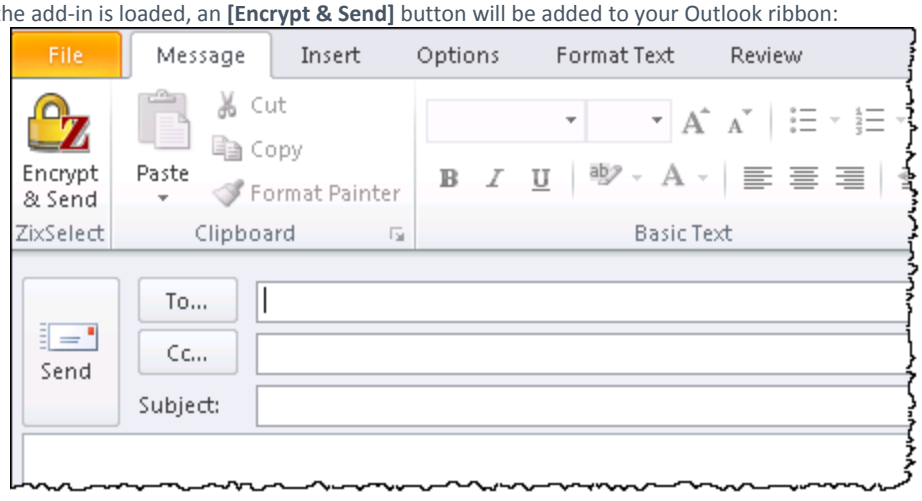
There are two ways to encrypt an e-mail message sent from the University E-mail Service:

Method 1: **Subject Line Phrase**

- Include the phrase "**[ucsecure]**" –brackets included, anywhere in the Subject of your message.
  This option will work with Outlook Web App (OWA) and any UC Irvine Health E-mail Service supported client.
- Because the encryption phrase is in the Subject line and will not automatically be removed, the message will be encrypted in any reply or forward sent from the UC Irvine Health E-mail Service.

Method 2: **[Encrypt and Send]** button

- This is only an option for Outlook 2003, 2007, and 2010.
- Once the add-in is loaded, an **[Encrypt & Send]** button will be added to your Outlook ribbon:



Be aware that if an e-mail string or conversation develops, you must click [Encrypt & Send] every time you reply in order for the new message to be encrypted, if necessary.

FAQ

How does the policy work to determine which emails get encrypted?

UC Irvine Health's Secure Mail provides HIPAA content recognition to facilitate HIPAA-compliance with PHI. It does so by searching for two categories one being personal identifiable information (patient ID number, subscriber ID number, social security number, etc.) and medical terms, medical conditions, etc. When a match is found in both categories, the message will be encrypted.

Why are we implementing secure messaging?

With the adoption of the Health Insurance Portability and Accountability Act (HIPAA), it is required that all communications containing Protected Health Information (PHI) be secured. PHI refers to information that identifies you with a disease or condition or test or treatment. Since e-mail communication between you and External Associates typically involves scheduling appointments with healthcare providers, we felt it was important to protect the confidentiality of that information, so that only YOU have access to the information.

What is secure messaging?

Secure Messaging is the process of sending encrypted e-mail messages using ZixCorp's Method of Delivery.

When will the e-mail message expire for the Recipient?

The ZixCorp service does not provide long-term storage for encrypted messages.

All messages, both read and unread, will expire and be deleted from the ZixCorp portal 30 days after they are sent.

If after 14 days a message is not read in the portal, both the sender and recipient will receive an automatic notification that the message has not been read.

If after 30 days a message is not read in the portal, the sender will receive a notification that the message has not been read before the message is deleted.

What is the maximum size of attachments?

Attachments are supported as part of the Compose, Forward and Reply actions. You can click on the Attach Files button and select the file(s) you wish to attach to the message. The maximum number of files that can be attached is 10, and their total file size cannot exceed 10MB.

How do I know if my message was sent securely?

If you send an encrypted message to recipient, the e-mail the recipient receives will provide instructions for accessing the encrypted message from the ZixCorp portal.