

Secure E-Mail at UNM Health Sciences Center

[How it Works](#)

[How to Encrypt E-Mail](#)

[Information for the Sender](#)

[Information for the Recipient](#)

[Receiving an Encrypted Reply](#)

[Summary](#)

[Secure Email Appropriate Use Guidelines](#)

[Support Info](#)

The University of New Mexico Health Sciences Center, UNM Hospitals and the UNM Medical Group use an e-mail encryption system to help protect the privacy and confidentiality of sensitive information (electronic Protected Health information [ePHI], Financial, Personnel Information or other confidential types of information such as HR details, client-attorney privileged information etc.) contained in e-mail and its attachments.

Regular e-mail sent over the internet can be easily intercepted and read by unauthorized individuals. Encrypting this information makes it significantly harder for unauthorized individuals to do so. Encryption also helps us meet regulatory obligations under HIPAA and National Institute of Standards of Technology (NIST) standards.

Encrypted e-mail is available to our users as an Opt-in service.

How it Works

Secure E-mail at UNMH/HSC/UNMMG works in the following manner:

The sender types in ***secure*** in the Subject field of the e-mail. The remainder of the e-mail can then be typed normally and any attachments required can be added.

The IronPort e-mail encryption appliance sees the tag ***secure*** and automatically encrypts the body and attachments of the outbound e-mail and sends it to the recipient as an encrypted attachment. Please note, the Subject field will not be encrypted, so senders of encrypted e-mail should not include sensitive information in that field.

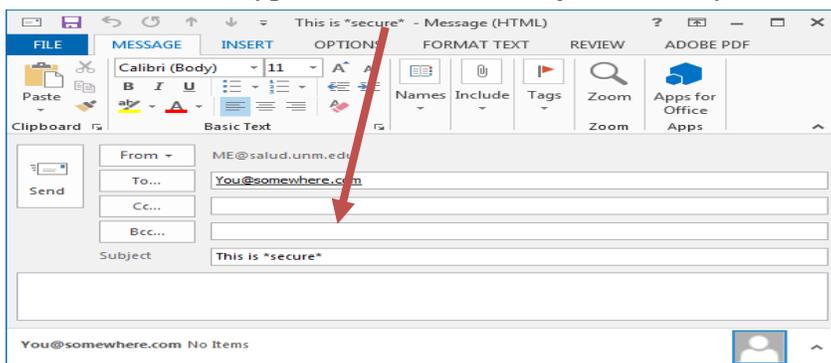
The recipient receives an e-mail notification that they have received an encrypted mail from someone at UNMH/HSC/UNMMG. This will include the word '[-Encrypted-]' at the end of the subject line.

The recipient opens the message's attachment and is prompted for their e-mail address and a password. This must be set up by the recipient using a one-time registration process at a third-party web site. They will only need to provide the e-mail address and password to open subsequent encrypted e-mails from UNMH/HSC/UNMMG staff.

For further details on how to [send](#) or [receive](#) encrypted e-mail please refer to the appropriate sections on this document.

How to Encrypt E-Mail

To encrypt an outbound e-mail, type ***secure*** in the subject field of your e-mail. An example is shown here:



Information for the Sender

When you send an encrypted e-mail using the process shown above, it will be sent just as any other e-mail message would be.

External Recipients (Outside of HSCLink):

The recipient will receive a message that will have [-Encrypted-] in place of *secure* in the subject.

Internal Recipients (Inside HSCLink):

The message will maintain the *secure* in the subject. However, your internal e-mail will not hit the outbound Ironport encryption appliance which sits at the periphery of our network and therefore will not be encrypted when sent to internal recipients.

Information for the Recipient

Recipients will receive a message such as the one shown here:

Palliative Care Consultation [-Encrypted-]

Inbox | X



James Bond to me

[show details](#) 8:38 AM (0 minutes ago)

[Reply](#)



You have received a secure message

Read your secure message by opening the attachment, [securedoc.html](#). You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. To access from a mobile device, forward this message to mobile@res.cisco.com to receive a mobile login URL.

If you have concerns about the validity of this message, contact the sender directly.

First time users - will need to register after opening the attachment. For more information, click the following Help link.

Help - <https://res.cisco.com/websafe/help?topic=ReqEnvelope>

About Cisco Registered Email Service - <https://res.cisco.com/websafe/about>

securedoc.html
108K [View](#) [Download](#)

[Reply](#) [Forward](#)

Open the encrypted attachment: **securedoc.html**. This will take you to a page which looks like this:

UNM
HEALTH SCIENCES
CENTER

CISCO REGISTERED ENVELOPE SERVICE

From: James Bond <jbond@salud.unm.edu>
To: jmoneypenney@mi6.gov.uk
Subject: Palliative Care Consultation [-Encrypted-]
Password:
[Forgot password?](#)

Personal Security Phrase
Your personal phrase is not enabled on this computer.
[More info](#)

Enter your password and click Open. If the Open button does not appear, forward the original email to mobile@res.cisco.com.

[Open](#)

New users, select your email address and click Open to create an account.

[My address is not listed](#)

Submit your password above to open your message online.

Cisco Registered Envelope Service

Copyright © 2000-2010 Cisco Systems, Inc. All rights reserved.

New users will need to select open to register their email account. Returning users can enter their password and then select open.

CISCO

English Help

YOU ARE NOT REGISTERED

To open this message, you must first register and create a password. To register, click on the link below or copy and paste it into your browser.
<https://res.cisco.com/websafe/register?uuid=0e4da97d0000012e25bc822dc0a86e8e609a05bf>

Cisco Registered Envelope Service

About Terms of Service Privacy Policy Copyright © 2001-2010 Cisco Systems, Inc. All rights reserved.

Internet | Protected Mode: On 100%

Click on the link shown in the message, above. This will take you to Cisco's new user registration window:

NEW USER REGISTRATION

To assure future messages from this service are not accidentally filtered out of your email, please add "DoNotReply@res.cisco.com" to your Address Book or Safe Sender List.

* = required field

Enter Personal Information

Email Address

Language

The language setting will be stored for future login and email notifications.

First Name*

Last Name*

Create a Password

Password*

Enter a minimum of 6 characters or numbers. Passwords are case-sensitive. Your password must contain both letters and numbers.

Confirm Password*

Personal Security Phrase*

Enter a short phrase that only you will know. This phrase will appear on message envelopes when you log in. When you see your phrase, you know you are logging in to our secure site. [More info](#)

Enable my Personal Security Phrase.

Select 3 Security Questions

You will be asked these questions in the future if you forget your password.

Question 1*

Answer 1*

Confirm Answer 1*

Question 2*

Answer 2*

Confirm Answer 2*

Question 3*

Answer 3*

Confirm Answer 3*



Fill in the details as requested on the registration page and select the Register button at the bottom. You will then see a screen like this one:

FINAL STEP: ACCOUNT ACTIVATION

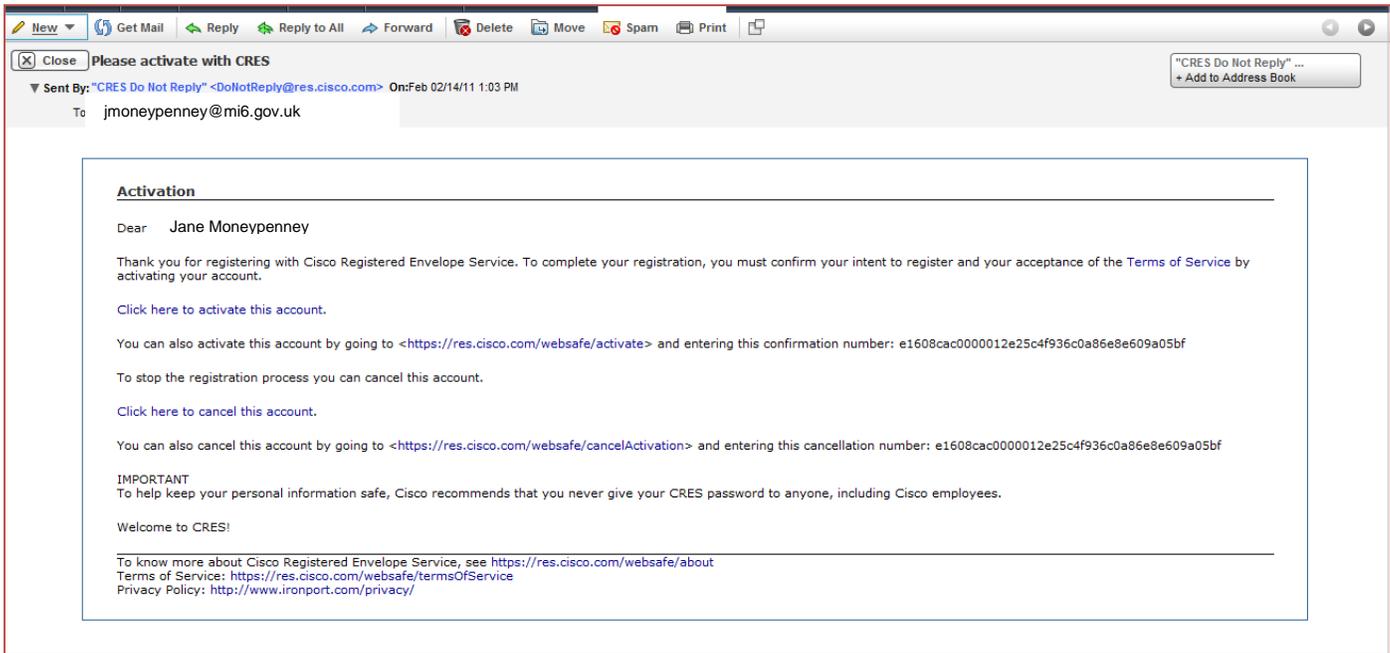
Your Cisco Registered Envelope Service account was successfully created.

Instructions to activate your account have been emailed to

@comcast.net.

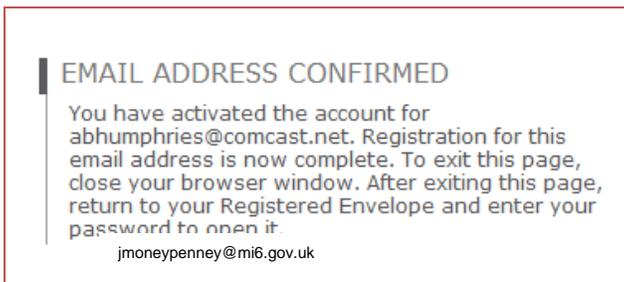
Please check your account folder.
Please check account folder.

Open the e-mail account where the instructions have been mailed to, and click on the message which looks like this (Sender is CRES; title of mail is 'Please Activate with CRES'):

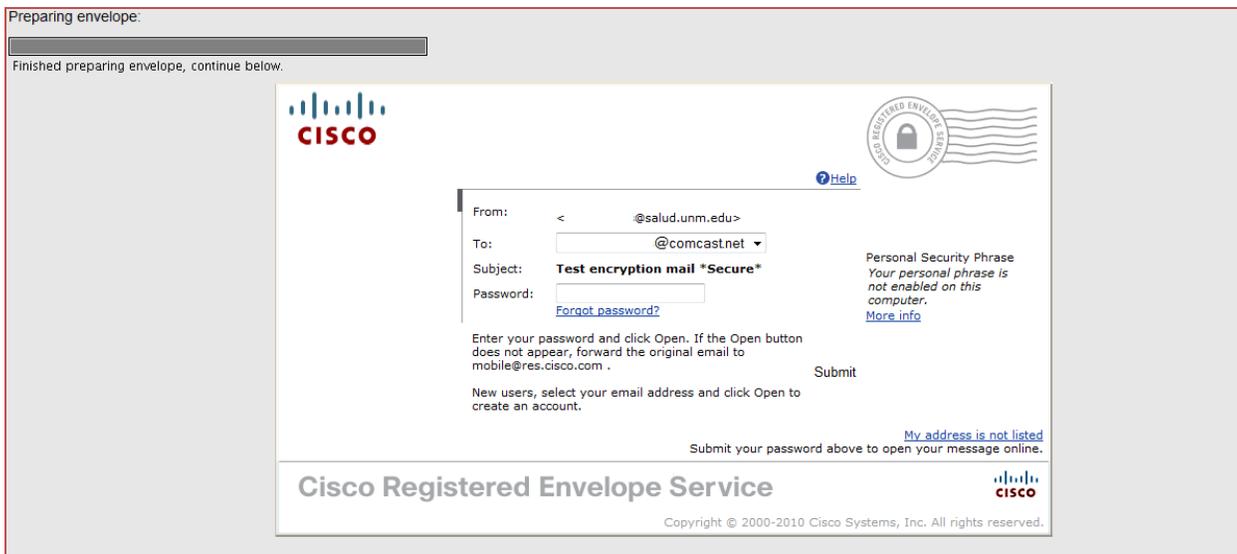


Click on the link which says “Click here to activate this account”.

This will take you to the confirmation page, as shown here:



You can then return to your e-mail account, and open the original e-mail message, click on the attachment and enter your password as shown here:



Once you have successfully entered your password and hit the Open button, the previously encrypted e-mail message will be displayed in clear text, as it is here:



The recipient can now reply as they would do with any normal mail e-message. These replies will also be encrypted. Recipients of encrypted confidential e-mail must maintain the security of the information by storing in approved areas.

Summary:

If you send out an e-mail with **secure** in the header to an **external** recipient (outside of UNMH/HSC/UNMMG) then **it will be encrypted**. If you send a message with **secure** in the subject field to a mixture of internal and external recipients, it will be encrypted need authentication. Internal recipients will not need to authenticate.

The **reply** from someone who has received an encrypted mail from you **will also be encrypted** but will automatically be decrypted by the Ironport device as it re-enters the HSC network. No further steps are required by you to read this reply. This will continue to apply to all subsequent replies also.

If you reply again, your reply will have **'Re:.....[-Encrypted-]'** (which automatically replaces **secure** when the mail is first sent out) in the title. Therefore **it will be encrypted again**.

Secure Email Appropriate Use Guidelines

Using email for business purposes requires compliance with applicable policies, procedures and departmental practices for handling Confidential information including electronic Protected Health Information (ePHI). These practices should be in line with the list below taken from the UNMH IT Security Email Use Procedures:

- Users must send only the minimal amount of EPHI information required to perform the task and ensure that they are sending to only an authorized recipient.
- Since the sender is responsible for the confidentiality of the message, extra care shall be exercised to insure that the message is properly addressed.
- E-mail shall only be used within the scope of a user's authorized function as assigned by UNM Hospitals or another branch of the University of New Mexico (UNM).

Any questions regarding whether data may appropriately be sent through email should be addressed to the user's direct supervisor and in line with departmental practices. Further assistance is available from a compliance, security or privacy officer.

Support Information

Users experiencing any issues or with questions concerning secure e-mail should contact their respective help desk.

Contact Details:

UNMH/UNMMG Helpdesk – (505) 272 3282 or HSLIC Helpdesk – (505) 272 1694