External Users - Decrypting Secure Messages

The following sections describe how users external to EJGH receive and decrypt secure messages.

Reading a Secure Message

When you receive a secure message, it will look similar to this in your mailbox:

Click the attachment *SecureMessageAtt.html* to launch a browser. Note: If the attachment looks like this 

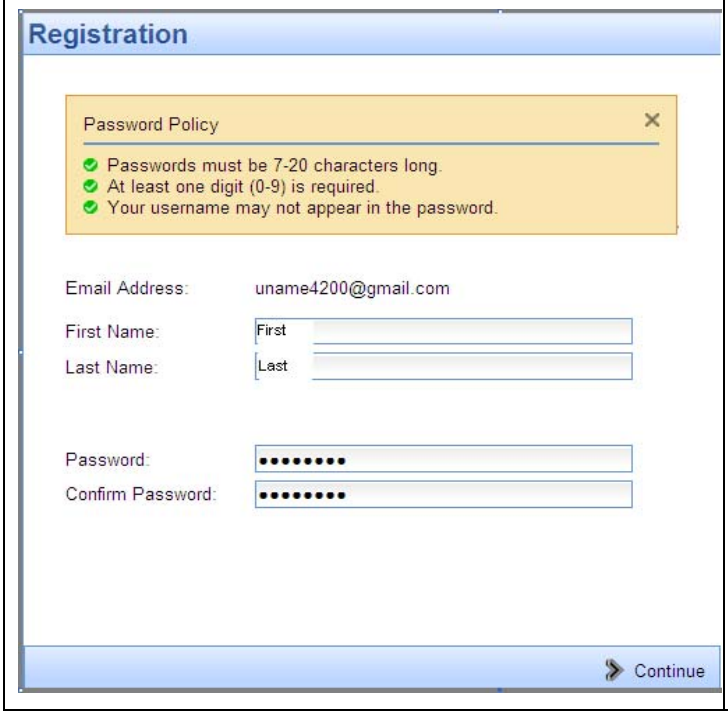
click Download and Open.

Open the Attachment

If this is the first time you are receiving an EJGH secure message at this email address, you will be prompted to create and confirm your new password. Otherwise, you will be prompted to log in using your password. Click the **Click to read message** button:

Create and Confirm Your Password / Log In to Receive Your Secure Message

Create and Confirm Your Password

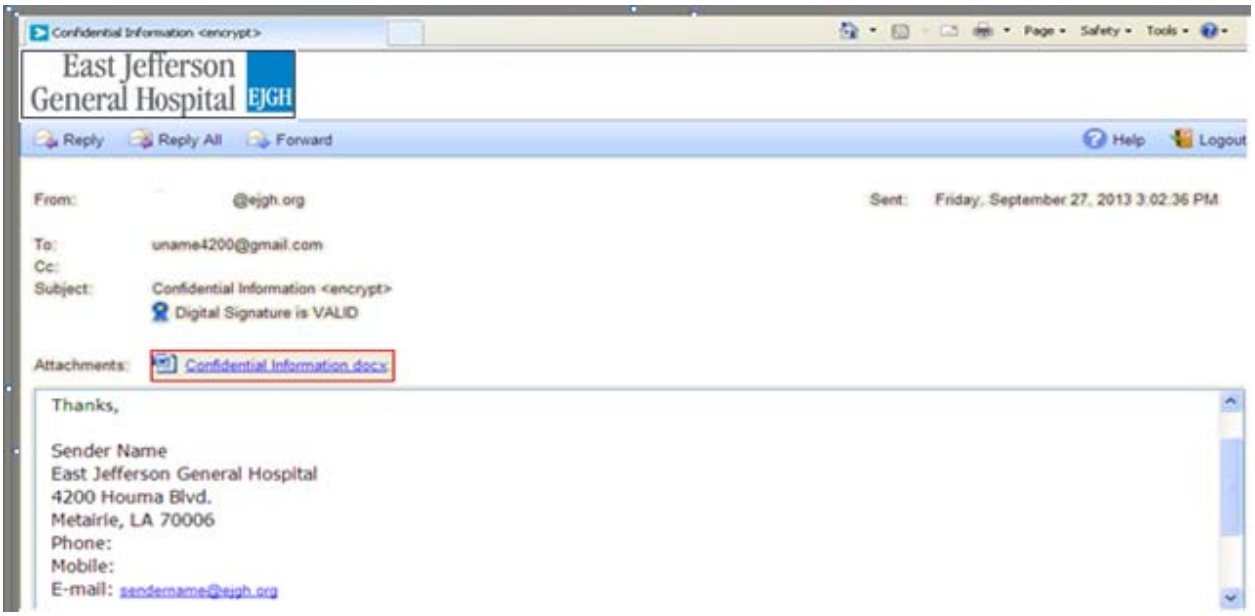


Log In to Receive Your Secure Message

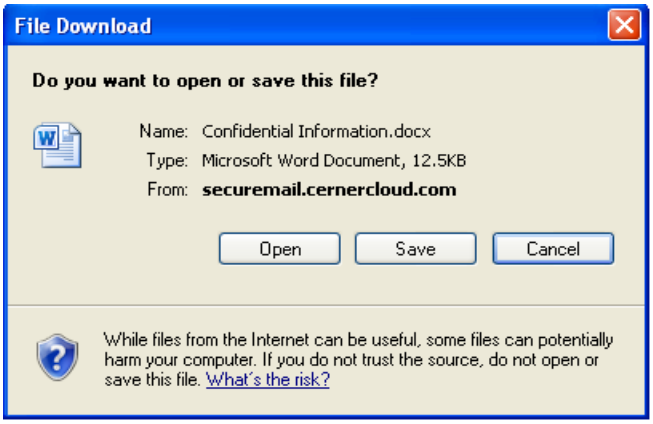
Fill in the fields, create and confirm your password using the above Password Policy, and then click **Continue**.

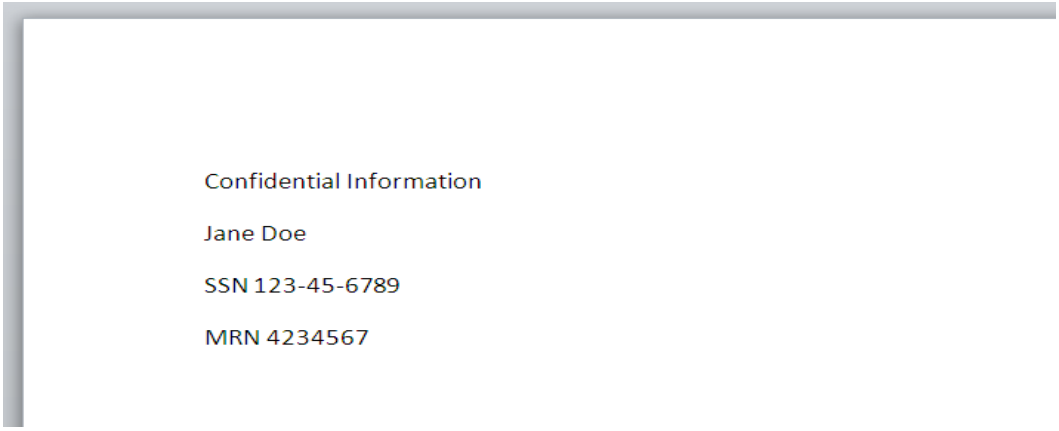
Read Your Message

The **Reply**, **Reply All**, and **Forward** options are available.



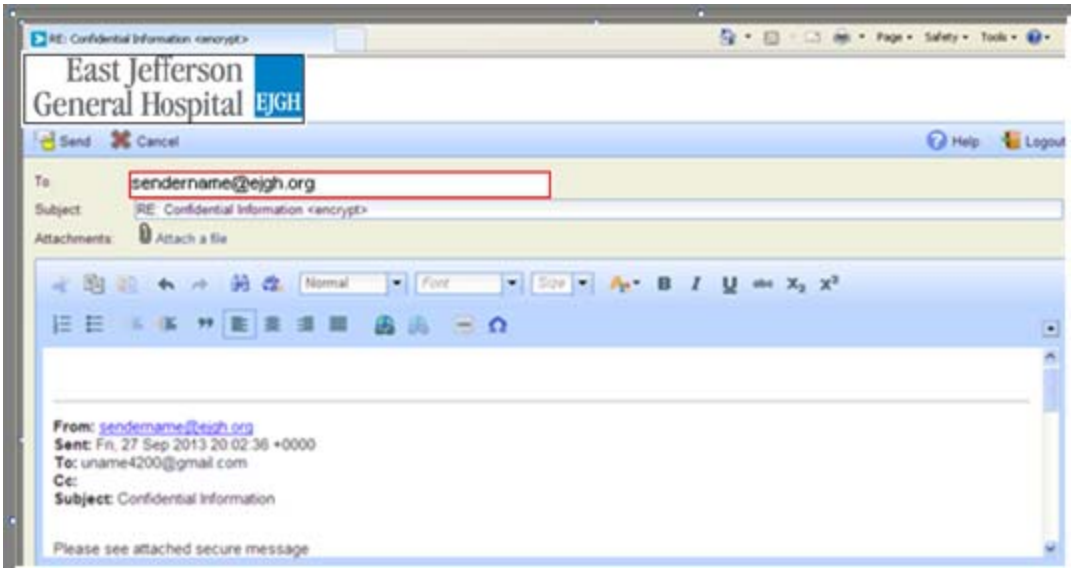
If an Attachment is shown to your secure message, click it and Open or Save:



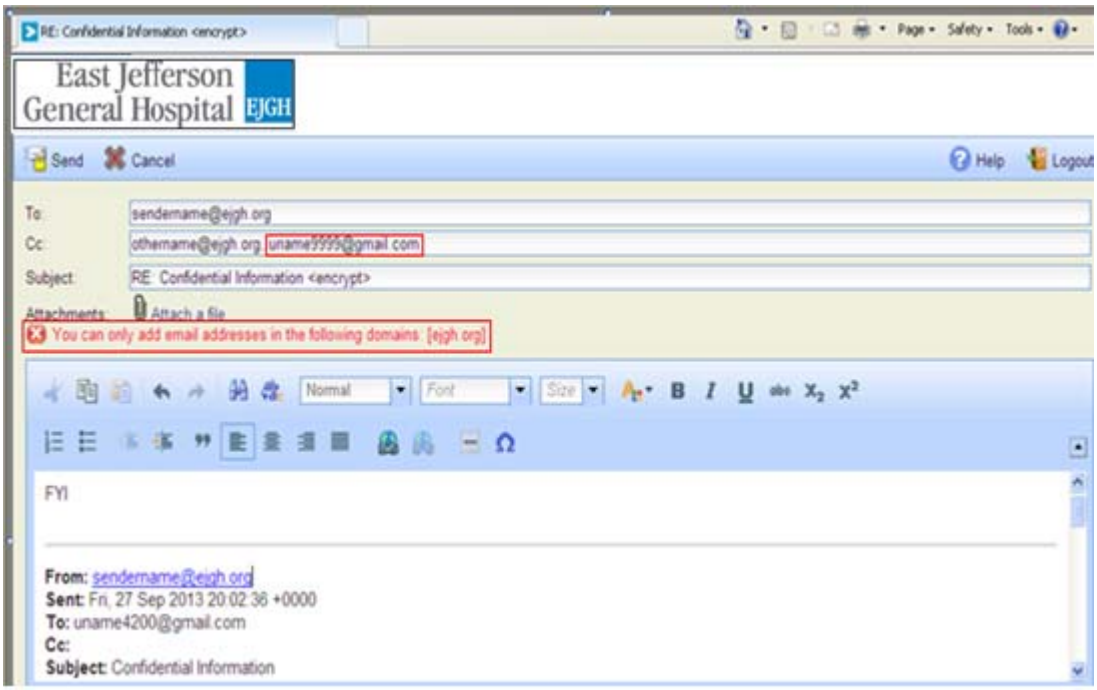


Reply, Reply All or Forward Your Message

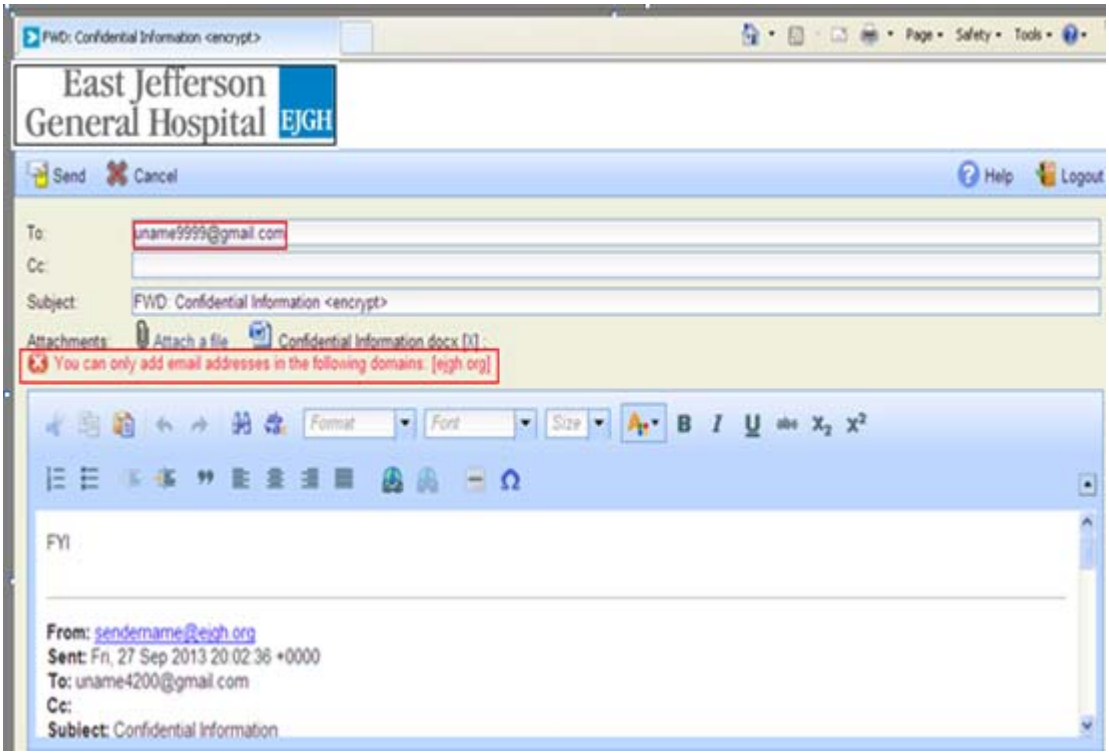
If you click **Reply** you cannot add more recipients to the message. You may add new attachments.



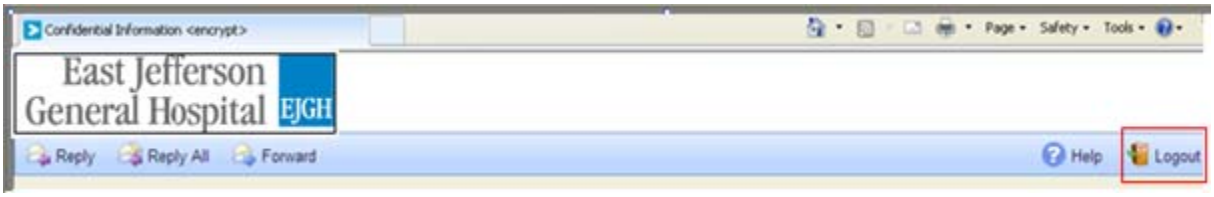
If you click **Reply All** you can add more recipients to the message; however, they are restricted to the original sender's domain. You may add new attachments.

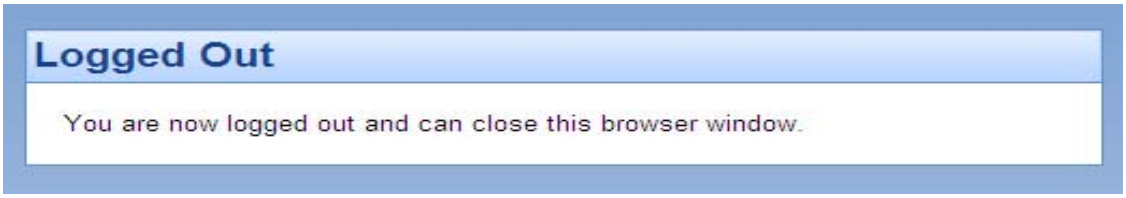


If you click **Forward** you can add recipients to the message; however, they are restricted to the original sender's domain. You may forward attachments received and add new attachments.



Click **Logout** when you are finished.

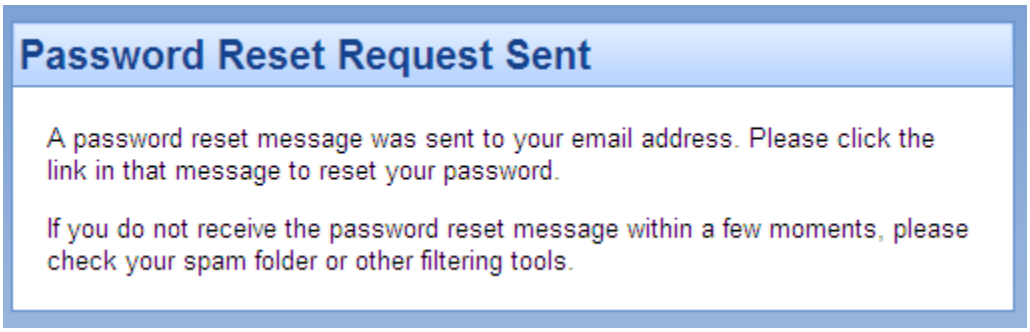




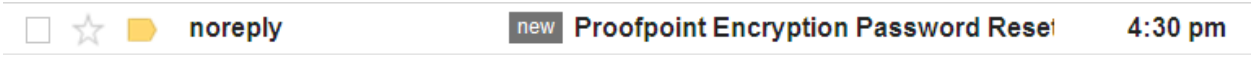
Forgetting Your Password

If you forgot your password, click the **Forgot Password** link.

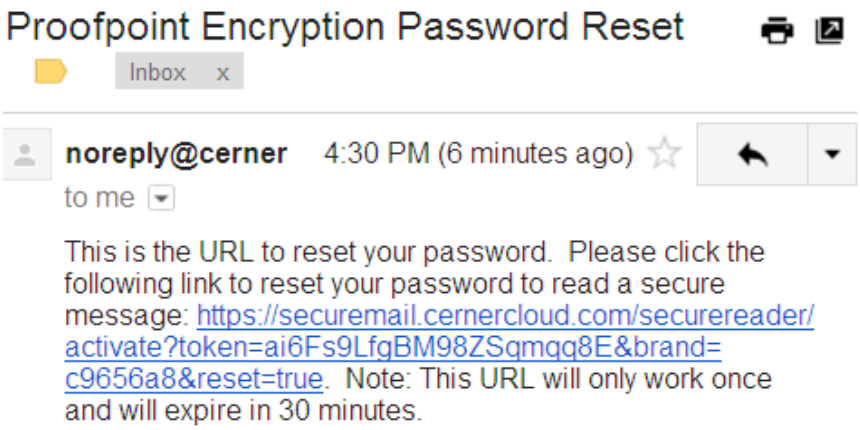
A pop-up message will inform you that a password reset message with a link has been sent to your email.



Locate and open the password reset message which looks like this:



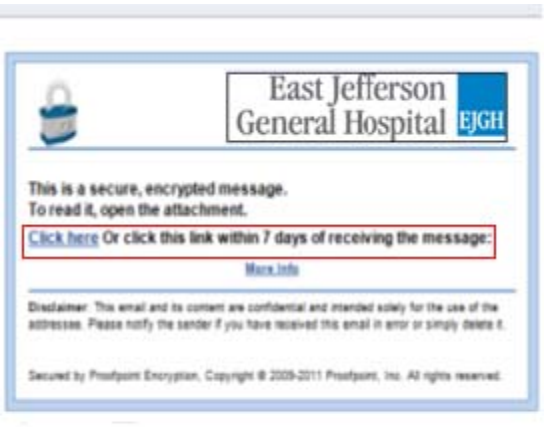
Click the link which will work only once and only for the next 30 minutes. If necessary you may go back to the original secure message and click through to the Login prompt and Forgot Password link.



Note: You are not required to change your password. If you incorrectly guess your password 5 times in succession, you will receive an Account Lockout message; however, the lockout is automatically reset after a short delay. Please use the self-service Forgot Password link to successfully retrieve your secure message.

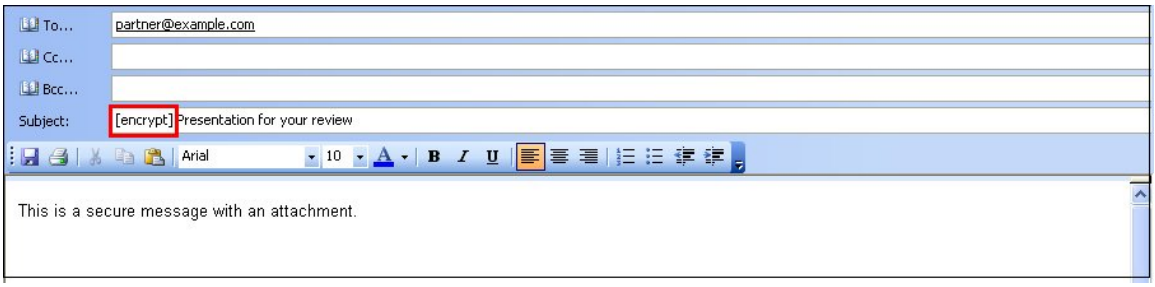
Decrypting Secure Messages from a Mobile Device

When you receive a secure message on your mobile device, it will include a web link available for 7 days:



Internal Users - Composing a Secure Message to External Users

When you want to send a secure message, all you need to do is use your regular email application and enter the word *[encrypt]* into the **Subject** field of your message. Include the square brackets.



When to Encrypt Email

All email that contains Personal Health Information or Business Confidential Information (collectively CI) is required to be encrypted per EJGH policy. All email will be electronically scanned and will be encrypted when such information is present. This is being done to help ensure that EJGH protects information privacy and security and to prevent unauthorized disclosure and release. Physicians, Allied Health Professionals, Team Members, and Contractors who use EJGH Outlook Email must only access or release the minimum amount of CI necessary to perform their job duties in association with treatment, payment and operations.

If a message must be sent to someone outside of EJGH and it contains CI, it must be encrypted by the sender. Please note: failing to encrypt an email going to destinations other than @ejgh.org that contains CI is a direct violation of EJGH policy.

To encrypt an email, the sender enters the ***<encrypt>*** command in the subject line before sending. If you omit the ***<encrypt>*** command and there is CI in the Body or in an attachment to the Email, automated encryption occurs. If CI is detected in the Subject line, it will be deleted and your Email sent. You will receive the Regulatory Compliance Alert as a reminder to always exclude CI before sending.

Recipients of your Email will also receive immediate notification of a secure message waiting for them. They will need to select the message link or attachment and follow the instructions to access and receive your message. If recipients should contact you regarding Email retrieval, it will help to advise them to follow the above instructions. A self-service Forgot Password link is available at the Login prompt, and account lockouts are automatically reset after a short delay.

Encrypted Emails are available to the recipient indefinitely. A web link for mobile devices is available for 7 days.

Questions may be addressed by contacting ITSecurity@ejgh.org or the HelpDesk@ejgh.org at 454-4847.

Encrypted Example

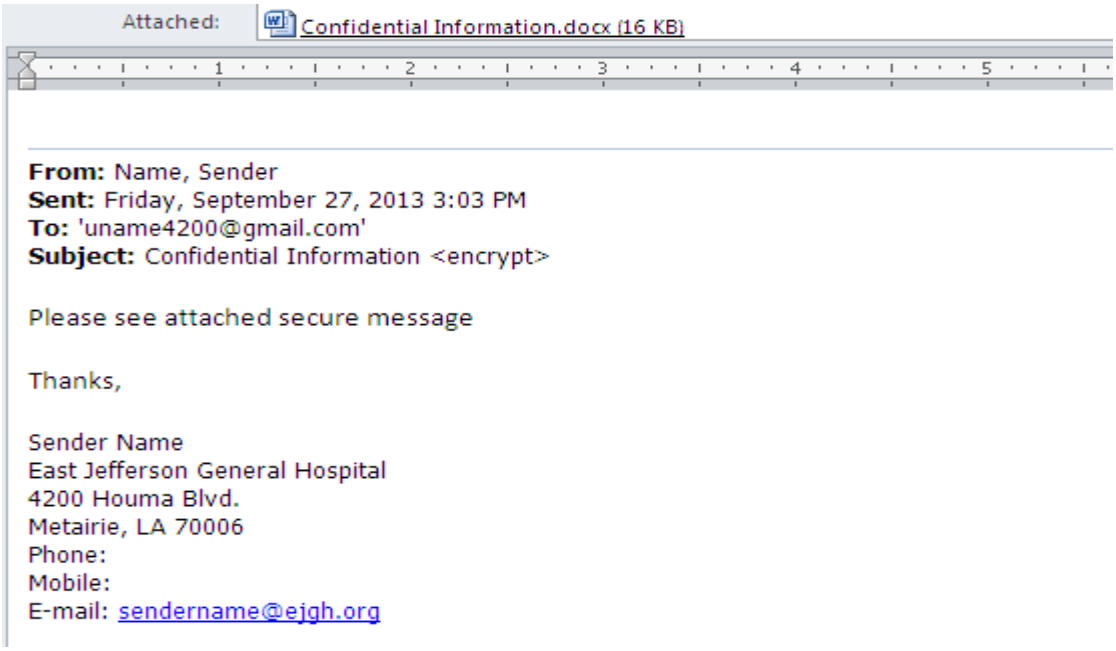
The example below is of a Word document with mock Confidential Information (CI), which was sent encrypted by EJGH Outlook Email to a destination other than @ejgh.org :

Confidential Information

Jane Doe

SSN 123-45-6789

MRN 4234567



Regulatory Compliance Alert Notification

The Regulatory Compliance Alert Notification identifies the Date, Time and Original Message Subject of the Encrypted Email containing Confidential Information (CI) sent to a destination other than @ejgh.org . The Alert reminds the sender that Confidential Information to recipients outside of EJGH requires encryption using the ***[encrypt]*** keyword and excluding CI in the Subject line before sending. If CI was detected in the subject line, it was deleted and your email sent.