Secure Email Gateway

Procedure

CBIS – Information Security Office
## Contents

Purpose .................................................................................................................................................. 2
Scope.................................................................................................................................................... 2
General Requirements.............................................................................................................................. 2
How do you encrypt emails using Secure Email? ................................................................................. 3
How do you access a UCMC encrypted email? ....................................................................................... 4
Additional information on Secure Email ............................................................................................... 8
**Purpose**
Secure Email service is provided to all UCMC departments using the UCMC Exchange email system. This service will assist the organization in meeting IT security compliance and regulatory requirements. The purpose of this document is to provide a step by step procedure for encrypting outgoing email, and receipt/decryption by external recipients.

**Scope**
The Secure Email service encrypts email sent to external recipients such as Hotmail, AOL, Gmail, in addition to UCMC business partners.

**General Requirements**
As per the HIPAA Security Rule requirement 164.312(a)(2)(iv), Protected Health Information (PHI) must be encrypted when sent over insecure channels, such as the Internet. UCMC extends this standard to include other highly sensitive data. Examples of highly sensitive data includes: Highly Confidential Information Information (HCI) or Personally Identifiable Information (PII). Examples of PII include a social security number, passport number, medical insurance number, credit card number and so on.

To help meet this requirement, UCMC CBIS provides the Secure Email services to all UCMC departments.
How do you encrypt emails using Secure Email?

1. To send encrypted emails to an external recipient (for example: Hotmail, Gmail, AOL, etc.) prepend #encrypt in the subject line, alongside your desired subject title.

2. The recipient will receive the email similar to the below screenshot.
How do you access a UCMC encrypted email?

When UCMC personnel send outbound mail (for example: to Hotmail, gmail, aol, etc.) with #encrypt in the subject line, the message is encrypted by the UCMC email systems and a notification is sent to the recipient.

1. The notification to external recipients is displayed below:

2. To open the message, you must open the “SecureMessageAtt.html” attachment or click on “Click here” link as shown in the above screenshot. “Click this link…” link takes 1-2 min to generate after the message is sent. In case you get a session timeout message, wait for few minutes and click again.

3. You will be asked to register to the secure email portal and will be asked to provide a password. Click “Continue” after populating the registration fields.
4. Using the newly created account you will be able to authenticate, as shown below.

5. The secure email portal decrypts the message and the message can be viewed.
Click **Logout** when you are done.
Please note –

- You are not permitted to forward the email to any contact other than those included in the original email.

- You can reply to the sender and others in the email.

- The email link (Click here) will expire in 7 days. To open the email after the link expires, download the attachment “SecureMessageAtt.html” and open the attachment using a browser such as Internet Explorer (IE) or Firefox.
Additional information on Secure Email

1. The secure email portal allows 8 attempts before the account is locked. If your account is locked out you will receive the following message. Your account will remain locked for 1 minute.

![Account Temporarily Locked Out]

2. If you forgot your password, you can reset the password by clicking on the “Forgot Password” button.

![Login Screen]

![Password Reset Request Sent]
3. A hyperlink will be emailed to you, assisting in the resetting your password.

4. You will then create a new password. A new browser window will be displayed to enter the new password.

5. If for any reason the password reset option does not work, please send an email to UCMC Service Desk at help@bsd.uchicago.edu from the email account that the secure message was received.