

UMMC Email Encryption

Automatic Encryption

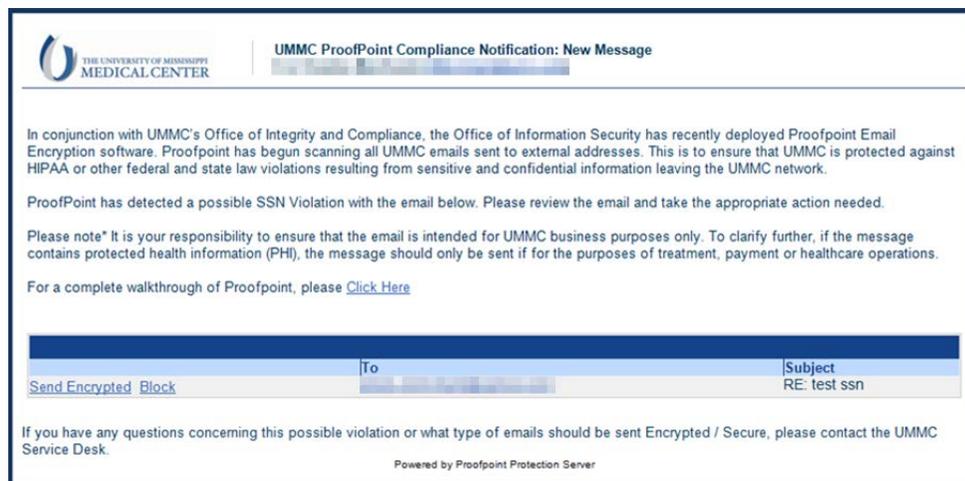
All messages to non-UMMC email addresses will be scanned for potential violations

- Numbers in the body of an email can trigger a violation including any number that looks like a social security number or other potentially sensitive information.

If the system detects a violation, you will receive a notification stating that there has been a possible violation and it will ask for your interaction.

Click **“Send Encrypted”** to encrypt and send the message.

Click **“Block”** to stop the message from being sent.



The screenshot shows an email notification from The University of Mississippi Medical Center. The header includes the UMMC logo and the text "UMMC ProofPoint Compliance Notification: New Message". The main body of the email contains the following text:

In conjunction with UMMC's Office of Integrity and Compliance, the Office of Information Security has recently deployed Proofpoint Email Encryption software. Proofpoint has begun scanning all UMMC emails sent to external addresses. This is to ensure that UMMC is protected against HIPAA or other federal and state law violations resulting from sensitive and confidential information leaving the UMMC network.

ProofPoint has detected a possible SSN Violation with the email below. Please review the email and take the appropriate action needed.

Please note* It is your responsibility to ensure that the email is intended for UMMC business purposes only. To clarify further, if the message contains protected health information (PHI), the message should only be sent if for the purposes of treatment, payment or healthcare operations.

For a complete walkthrough of Proofpoint, please [Click Here](#)

Below the text is a table with three columns: "Send Encrypted", "Block", and "Subject". The "Subject" column contains the text "RE: test ssn".

At the bottom of the email, it says: "If you have any questions concerning this possible violation or what type of emails should be sent Encrypted / Secure, please contact the UMMC Service Desk." and "Powered by Proofpoint Protection Server".

After sending an encrypted email, your non-UMMC recipient will receive the following dialog box:
The recipient must click on the **“Click here”** link to open the encrypted document.



The screenshot shows a dialog box with a blue border. On the left is a padlock icon, and on the right is the UMMC logo. The text inside the dialog box reads:

This is a secure message.
[Click here](#) by 2012-10-31 08:53 CDT to read your message.
After that, open the attachment.

Below this is a link for [More Info](#).

A disclaimer follows: "Disclaimer: This email and its content are confidential and intended solely for the use of the addressee. Please notify the sender if you have received this email in error or simply delete it."

At the bottom, it says: "Secured by Proofpoint Encryption, Copyright © 2009-2012 Proofpoint, Inc. All rights reserved."

UMMC Email Encryption

This will open a registration dialog box where they must enter their first-name, last-name, and a password. The password requirements will appear as they type.



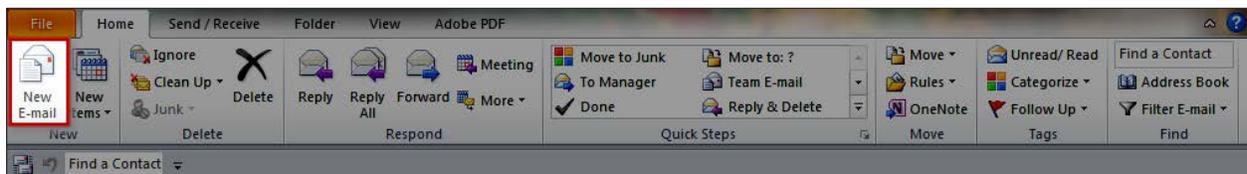
The registration dialog box is titled "Registration" and features the UMMC logo at the top. It contains the following fields:

- Email Address: [Redacted]
- First Name: [Text Input]
- Last Name: [Text Input]
- Password: [Text Input]
- Confirm Password: [Text Input]

A "Continue" button is located at the bottom right of the dialog.

Forcing Encryption

If you would like to force an encrypted email, first click on the “New Email” icon.



Next, simply type **[secure]** anywhere in the subject line. It is not case-sensitive and must include the brackets [].



The screenshot shows the "New Email" form in Outlook. The "Subject" field contains the text "[secure]". The "To...", "Cc...", and "Bcc..." fields are empty. A "Send" button is visible on the left side of the form.

If you need additional assistance, contact the Service Desk at 4-1145 or visit <http://servicedesk.umc.edu>

UMMC Email Encryption

Frequently Asked Questions

Do I need to force encryption since the system is automatically scanning the emails?

Yes. Scanning is just one layer of protection from UMMC. It is still up to the user to protect UMMC information and data.

Is it okay to send Patient Health Information via email externally as long as I force encryption?

No. Patient Health Information should only be sent outside of UMMC under limited circumstances. It is the sender's responsibility to ensure that the email is sent for appropriate purposes. If you have questions regarding the appropriateness of sending patient health information via email, please contact the Office of Integrity and Compliance at 5-3944.