# UMMC Email Encryption

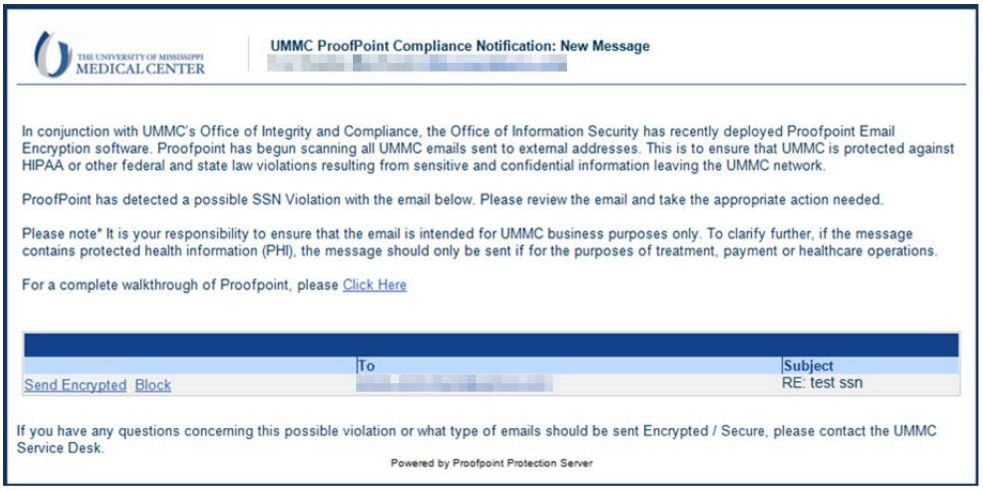
## Automatic Encryption

**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.



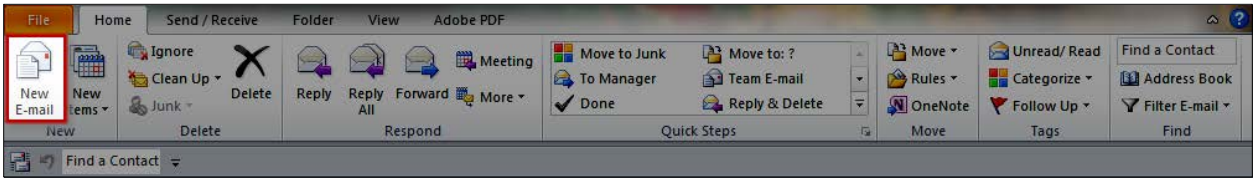

After sending an encrypted email, your non-UMMC recipient will receive the following dialog box:
The recipient must click on the "**Click here**" link to open the encrypted document.

# 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.


## 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 [ ].


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.