



How to Encrypt an Email

When and why should I encrypt an email?

When sending an email that contains **Protected Health Information (PHI)** or **confidential information**, you should **always** encrypt the email you are sending.

When you encrypt an email, the readable plain text is scrambled into a cipher text. This means that only the recipient can decipher it. If your encrypted email is intercepted or received by anyone other than the intended recipient, they will only see indecipherable text.


By encrypting an email, we are ensuring that we protect confidential information, especially PHI.

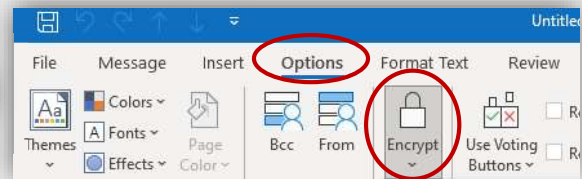
How do I encrypt an email?

From **Outlook**, the **desktop** version, follow these steps:

1. Click **New Email** as you would normally to compose an email
2. Select the **Options Tab** from the **New Message Menu**
3. Click on the **Encrypt Icon**



 Encrypt-Only - This message is encrypted. Recipients can't remove encryption.




Remember, the email **Subject Line** should **NEVER** contain **PHI** or **confidential information** because this field is always visible.



From **Outlook 365 (online version)**

1. Click **New Message** as you would normally to compose an email
2. Click on the **Encrypt Icon**



 Encrypt: This message is encrypted. Recipients can't remove encryption. [Change permissions](#) | [Remove encryption](#)

Important Things to Remember When Sharing Confidential or Protected Health Information (PHI)

1. Confirm that **you have authorization** to disclose the requested information.
2. Only **share the minimum** amount necessary to satisfy an information request.
3. When saving a file, **do not include PHI in the naming convention**.
4. **Do not include any PHI in the subject line** of the message because this field is always visible.
5. Review and **verify** that you are **sharing the correct file**.
6. **Verify** that you have the **correct recipient** and email address.
7. **Verify** that the file was **received** and accessed by the **intended recipient**.
8. If the information was **disclosed without authorization**, **contact the Compliance & Privacy Officer** to report the incident.