



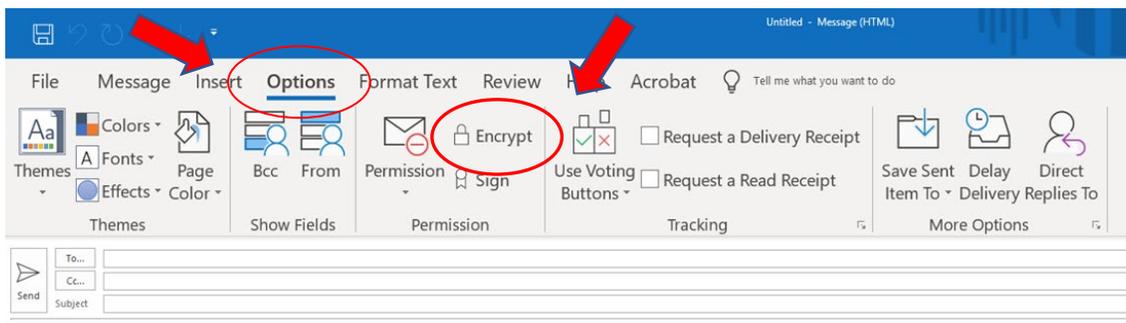
## Monday Morning Practice Pearls # 59

### What are my options to send secure email?

There are **four** ways to use secure communication: Encrypted Email, Secure Email and File Transfer (SEFT), Secure Health Messaging (SHM), and Medical Secure Email.

#### Encrypted email

- Used through a Microsoft Outlook account
- Requires PIV card



#### Secure Email and File Transfer (SEFT)

- Allows NIH users and its customers to send email securely and confidentially over an encrypted connection with or without large files
- Available via website <https://secureemail.nih.gov>

#### Secure Health Messaging (SHM)

- Preferred mechanism for securely messaging other NIH staff about patients
- Can be used to securely communicate with other CRIS users
- Messages can be attached to a patient's medical record
- Training materials available on the CRIS website

[https://cris.cc.nih.gov/cristraining/training\\_materials.html#secure\\_health\\_messaging](https://cris.cc.nih.gov/cristraining/training_materials.html#secure_health_messaging)

#### Medical Secure Email

- Can be used to securely communicate with patients
- Allows attachment of files outside of CRIS
- Available via website <https://medicalsecureemail.nih.gov/>

### Resources

Health Information Management Department (HIMD) website:

<http://intranet.cc.nih.gov/medicalrecords/index.html>

[HRPP SOP 18: Privacy and Confidentiality](#)- NIH follows federal law provided by the Privacy act of 1974

Mobile device- must be enrolled with MobileIron in order to send and receive encrypted email  
[https://service.cancer.gov/ncisp?id=kb\\_article\\_view&sysparm\\_article=NCI-KB0013608](https://service.cancer.gov/ncisp?id=kb_article_view&sysparm_article=NCI-KB0013608)

NIH Clinical Center (CC) Secure Communications

[http://intranet.cc.nih.gov/medicalrecords/pdf/NIH\\_CC\\_Secure\\_Communications.pdf](http://intranet.cc.nih.gov/medicalrecords/pdf/NIH_CC_Secure_Communications.pdf)

NIH policy [M09-3\(rev\)](#) states that any Personally Identifiable Information (PII) must be protected by encryption during transmission to protect the confidentiality of the information.

Requests and FAQs for Secure File Transfer (via Outlook)

<https://ees.sps.nih.gov/services/Pages/secureFiletransfer.aspx>