



Monday Morning Practice Pearls # 59

What are my options to send secure email?

There are **five** ways to use secure communication: Secure Health Messaging (SHM), Medical Secure Email (MSE), Encrypted Email, Secure Email and File Transfer (SEFT), and Office 365 Message Encryption (OME).

IMPORTANT: Communications with patients can only be done via SHM or MSE.

Secure Health Messaging (SHM)

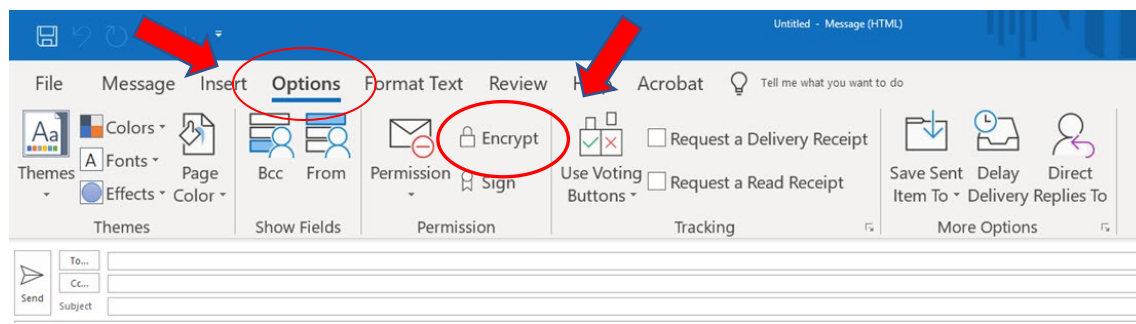
- Can be used to securely communicate with patients
- Preferred mechanism for securely messaging other NIH staff about patients
- Can be used to securely communicate with other CRIS users
- Messages can be attached to a patient's medical record
- Training materials available on the CRIS website
[https://cris.cc.nih.gov/cristraining/training_materials.html#secure 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/>

Encrypted email

- This method is not allowed to be used to communicate with patients
- Used through a Microsoft Outlook account
- Requires PIV card



Secure Email and File Transfer (SEFT)

- This method is not allowed to be used to communicate with patients
- 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>

Office 365 Message Encryption (OME)

- This method is not allowed to be used to communicate with patients
- Ability to send and receive encrypted emails inside AND outside of the NIH network without using a PIV card
- For detailed information, click here: [Office 365: Sending email using Message Encryption \(OME\)](#)

Resources

- Health Information Management Department (HIMD) website:
<http://intranet.cc.nih.gov/medicalrecords/index.html>
- [NIH HRPP Policy 107-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
- NIH Clinical Center (CC) Secure Communications
http://intranet.cc.nih.gov/medicalrecords/pdf/NIH_CC_Secure_Communications.pdf
- [NIH Clinical Center 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>