**To originate an encrypted email transmission you <u>must</u> use your official @etsu.edu email address. External email and Goldmail accounts are <u>not</u> equipped with encryption service and cannot be used to transmit or receive protected health information as they are not hosted by ETSU or covered under ETSU compliance contracts. For these same reasons your official @etsu.edu account should <u>not</u> be forwarded to external email or Goldmail account.

**The rules below apply for communications of protected health information by and between members of the healthcare team. Separate rules apply for communication with patients (i.e., patients receive *un*encrypted email <u>after</u> they sign a consent form).

ALL EMAIL COMMUNICATIONS BY AND BETWEEN THE HEALTHCARE TEAM THAT CONTAIN PROTECTED HEALTH INFORMATION <u>MUST</u> BE ENCRYPTED.

How do I encrypt email?
Internal Email Communications (@etsu.edu to @etsu.edu):
1. Simply type the word encrypt anywhere in the subject line to encrypt the contents of the message and the message attachments
2. Do *not* include protected health information in the subject line as the subject line itself is *not* secure

Encrypted messages sent internally will show up in the ETSU inbox and look completely normal—no actions have to be taken to decrypt/read the message
When the recipient takes subsequent action with an encrypted email (e.g. replies or forwards it) the subsequent emails will remain encrypted so long as the trigger word—encrypt—remains in the subject line

---

External Email Communications (etsu.edu to external address)
1. Simply type the word encrypt anywhere in the subject line to encrypt the contents of the message and the message attachments
2. Do *not* include protected health information in the subject line as the subject line itself is *not* secure

Encrypted messages sent from an etsu.edu address to an external address will show up in the recipient's mailbox and require extra steps—recipient will have to follow instructions to access contents of the encrypted message within a secure portal session
When the recipient takes subsequent action with an encrypted email (e.g. replies or forwards it) the subsequent emails will remain encrypted so long as all actions are taken within the secure portal session

Example:
An etsu.edu user sends an encrypted email to an external MSHA email address by typing the word encrypt in the subject line. The MSHA recipient will receive an email that says: "You've received an encrypted message from <u>username@etsu.edu</u>." To actually read the content of the message the MSHA recipient has to click a link and verify they are who they say they are by entering a code that Microsoft auto generates for them. The actual message content then opens inside a secure portal session. Actions taken by the MSHA recipient inside the secure portal will remain encrypted.

Visual Aids:

Summary of Email Rules

Email with Providers, Staff and members of the healthcare team	Email with Patients
✓ *Originates* from your @etsu.edu email account ✓ Trigger word encrypt in the subject ✓ No PHI in the subject Email must be encrypted. Encrypt must remain in the subject line when replying, forwarding, etc.	✓ *Originates* from your @etsu.edu email account ✓ Risks explained and signed consent obtained *prior to* emailing with the patient Email with patients is <u>unencrypted</u>. PHI may be sent via email once patient consent is obtained.

FILE   MESSAGE   INSERT   OPTIONS   FORMAT TEXT   REVIEW

Paste — Cut, Copy, Format Painter | Clipboard | Arial Narro ▾ 12 ▾ A⁺ A˅ | B I U | Basic Text | Address Check Attach

To... **Lindsay Daniel**

Cc...

Subject **Schedule Updates** Encrypt

This email satisfies the HIPAA email requirements!
✓ **Email originates from @etsu.edu address**
✓ **Trigger word encrypt in the Subject Line**
✓ **No PHI in Subject Line**

Lindsay,

Patient John Smith, DOB 04-11-1992 cancelled his afternoon appointment. I scheduled Patient Andrea Roberts, DOB 01-19-1986 in his place.