

EMAIL ENCRYPTION

ENCRYPTING EMAIL WHEN SENDING PHI

I. ASSOCIATED POLICY

CEHS HIPAA Policy 9000- Transmission Security

II. PURPOSE

All email transmissions containing sensitive information, including ePHI, must be encrypted before sending. Integrity Controls have been implemented by CEHS IT to ensure security of email transmissions between sender and receiver. This includes email transmissions that originate from senders within the SCCE to receivers both in and outside of the SCCE.

This process sheet has been created to help ensure emails are encrypted consistently to reduce risk of a breach.

III. PROCEDURES

The following steps must be taken to enable email encryption when required:

A. Use only CEHS approved devices and email accounts

Emails containing ePHI must be sent from CEHS IT approved devices only. Cell phones are not approved devices to send ePHI as encryption is not available within these Outlook applications. USU email accounts (@usu.edu) are the only accounts that USU business may be conducted with. Non-usu.edu accounts may not be used nor can usu.edu email be forwarded to a personal email account.

Before sending ePHI, email accounts should be set up with a signature to include the following privacy statement:

WARNING: CONFIDENTIALITY NOTICE- The information enclosed with this transmission may contain privileged and confidential information. It is intended solely for the individual(s) indicated. If you are not the intended recipient, you are notified that any review, disclosure, copying, distribution, or the taking of any other action relevant to the contents of this transmission are strictly prohibited. If you have received this transmission in error, please contact the sender by reply email immediately and destroy all copies of the original message.

B. Authenticate receiver

Reasonable safeguards must be taken to ensure the email is being sent to the correct individual. This may be done by sending a test email to the individual and confirming receipt before sending an email containing ePHI.

C. Encrypt email within Outlook

All USU email accounts have an option to encrypt within Outlook. Directions are included for both online (OWA) and desktop versions of Outlook used on Mac and Windows devices. See the tables below for step by step directions within each application.

To determine which Microsoft Office version (365 or 2019) is being used on your device:

MacOS	From main Outlook screen: • Click Outlook from main menu • Select About Outlook • Account information will be displayed, refer to “License Information”
Windows	Within the desktop version of Outlook: • Click File • Select Office Account • Account information will be displayed on the right, refer to “Product Activated”

Note: If you have any difficulty accessing the following encryption options, please reach out to Don Gustafson as your Microsoft version and/or license may need to be updated.

MacOS	
Desktop Office 365 and Office 2019	<u>Starting a new message:</u> • Begin by drafting a new email • Select the Draft menu • Next, select Encrypt (see Note) • Select Do Not Forward as the type of encryption <u>Encrypting a message already written:</u> • Click on the Options tab while in the drafted message • Select the Encrypt ribbon button • Select Do Not Forward as the type of encryption NOTE: A DUO authentication may be required should verify permissions be shown within the Encrypt flyout menu section. Authenticate by selecting that option should it appear.

OWA Office 365 using Chrome browser	<u>Encrypting a new or existing message:</u> • Begin by drafting a new email • Select the Encrypt button at the top of the email message in progress • A message will appear at the top of the email stating the email is Encrypted. To change the type of encryption, click on Change Permissions. A box will populate with pull down options. • Select Do Not Forward as the type of encryption
Windows	
Desktop Office 365	<u>Starting a new message:</u> • Begin by drafting a new email • Select the File menu • Next, select Encrypt • Select Do Not Forward as the type of encryption <u>Encrypting a message already written:</u> • Click on the Options tab while in the drafted message • Select the Encrypt ribbon button • Select Do Not Forward as the type of encryption <u>To set an expiration date for the message:</u> • Click on the Options tab while in the drafted message • Select [...] option • Select Message Options... in the pull-down list • A box will populate with information • In the Delivery options section, click the Expires after box and enter the date and time you wish the email to no longer be accessible. NOTE: <u>DO NOT change Security Settings</u> as it may make the email undeliverable.
Desktop Office 2019	<u>Starting a new message:</u> • Begin by drafting a new email • Select the File menu • Next, select Restrict permissions to this item • Select Do Not Forward as the type of encryption

	<u>Encrypting a message already written:</u> • Click on the Options tab while in the drafted message • Select the Permission ribbon button • Select Do Not Forward as the type of encryption <u>To set an expiration date for the message:</u> • Click on the Options tab while in the drafted message • Select More Options fly out arrow • A box will populate with information • In the Delivery options section, click the Expires after box and enter the date and time you wish the email to no longer be accessible. NOTE: <u>DO NOT change Security Settings</u> as it may make the email undeliverable.
OWA Office 365 using Chrome browser	<u>Encrypting a new or existing message:</u> • Begin by drafting a new email • Select the Encrypt button at the top of the email message in progress • A message will appear at the top of the email stating the email is Encrypted. To change the type of encryption, click on Change Permissions. A box will populate with pull down options. • Select Do Not Forward as the type of encryption

D. Telehealth Zoom Appointments

Meeting invites are not able to use encryption. If Telehealth Zoom meetings are scheduled, and used to populate the Outlook calendar, they will need to be copied into a standard email, encrypted, then sent to recipients.

E. Incident Reporting

If an email containing ePHI is sent without encryption, an incident report must be completed. Report all incidents to the Privacy Officer: Joni Black at joni.black@usu.edu.