Texas Tech University Health Sciences Center El Paso
HIPAA Privacy Policy

Office of Institutional Compliance

Policy: HPP 4.3	Effective Date: May 18, 2016
Release of Protected Health Information by Email	Last Revision Date: ~~January 25, 2022~~ March 19, 2024
References: ~~http://www.hhs.gov/ocr/hipaa~~ https://www.hhs.gov/ocr/index.html	

Policy Statement

It is the policy of Texas Tech University Health Sciences Center El Paso (TTUHSC El Paso) to ensure the confidentiality of protected health information (PHI) released by email. This policy defines the minimum guidelines and procedures ~~that~~ individuals must follow when transmitting patient information via email. Unless otherwise allowed by federal or state law, TTU~~S~~HSC El Paso shall only email PHI as outlined in this policy.

Scope

This policy applies to all PHI maintained by TTUHSC El Paso.

Policy

PHI is allowed in internal messages without encryption, i.e., the email must go to another ttuhsc.edu email address.

Transmission of PHI to external parties, i.e., any email address other than ttuhsc.edu or ttu.edu, must be manually encrypted. This includes emails to patients, providers, hospitals, payors, etc.

How to manually encrypt email: Type **[send secure]** or **[ss]** in the subject line right before the subject of the email, as shown below.
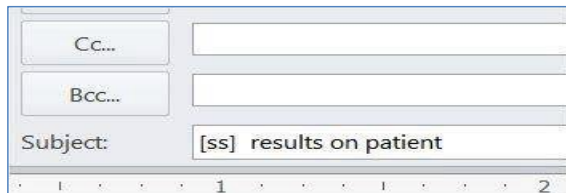
Transmission of PHI through EMR ~~— user may send secure messages via AthenaFlow EMR. This is the preferred method to send PHI. Steps:~~ The user may send secure messages via AthenaFlow EMR, which is the preferred method for sending PHI. The steps are outlined below.

1. Within the patient chart, select the Update button on the patient chart

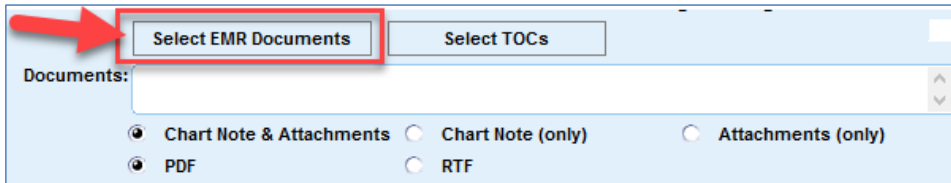2. Find and select "Secure Message to Patient" as an encounter

3. The SM Advanced form generates – each section is identified with a corresponding letter.

The provider/staff would complete the form as follows:

a) Recipient. The clinical team selects the patient as the recipient.

b) Subject and Body of the message.

c) Attachments that may be added to the message.

To attach clinical documents to the message, choose the Select EMR Documents button.

Based on the Document ID in EMR, select the corresponding Document ID from the Patient Attachments box. Then click "Select and Close."

The selected document will then show in the documents area within the form.
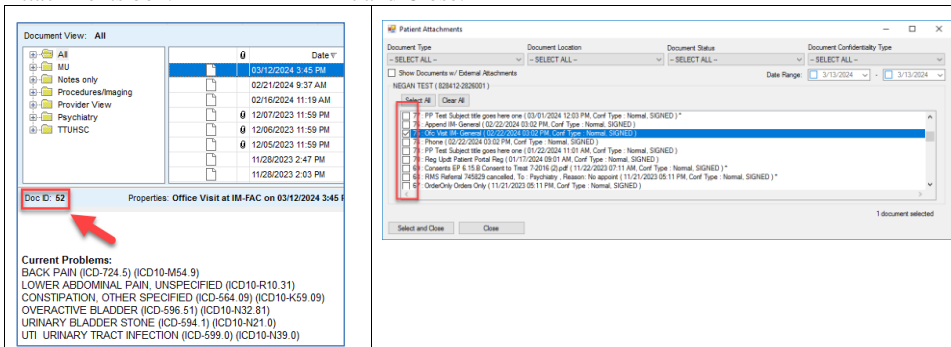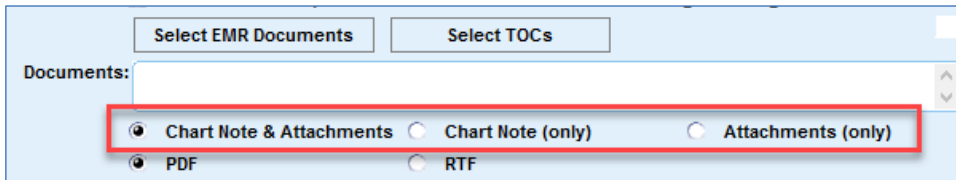
The sender may elect to send the Chart Note & Attachments, Chart Note (only), or Attachments (only).

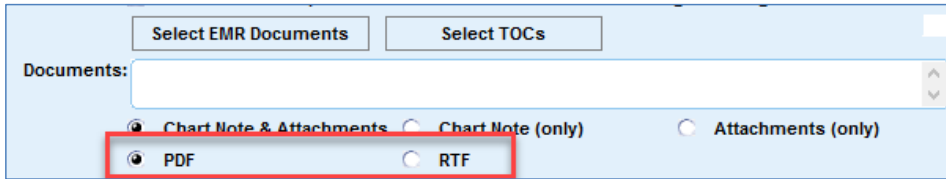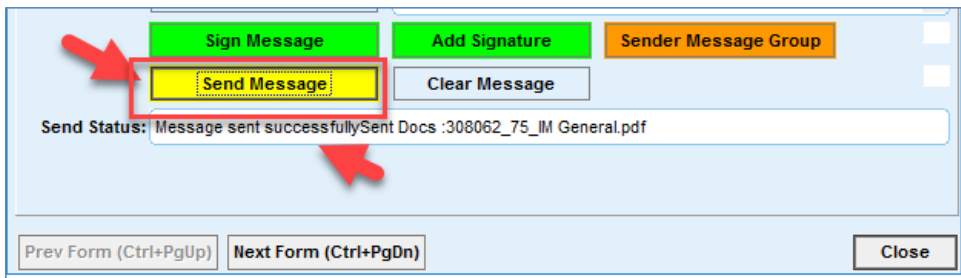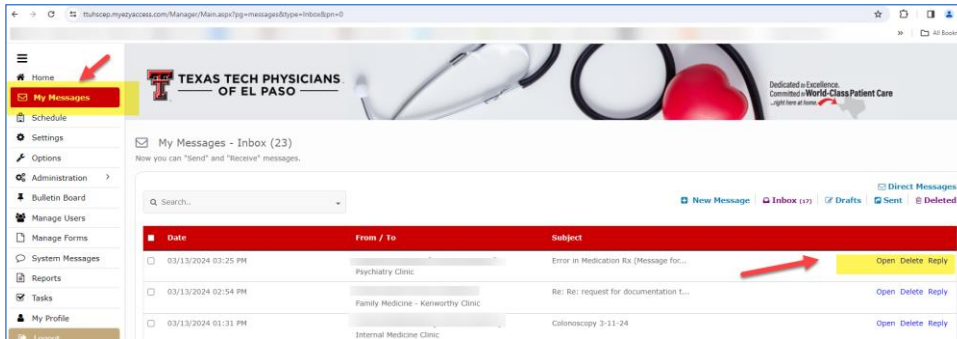In addition, the user may choose to send the documents as either a "PDF" or "RTF" file.

Click "Send Message" to transmit the message to the patient's portal. If the message is sent successfully, a timestamp will be added in the box underneath the "Send Message" button.

Staff members designated to manage incoming messages from patients can review patient replies in the portal by logging in.

If a patient requests in writing that their PHI be sent unencrypted, TTUHSC El Paso will inform the patient of the risks associated with ~~sending PHI unencrypted~~ doing so. However, if the patient insists, TTUHSC El Paso will comply, documenting the patient's request in their record.

> **Commented [QY1]:** Should we remove this because the patient has the right to request it in the format.

Knowledge of a violation or potential violation of this policy must be reported directly to the

Institutional Privacy Officer or the Fraud and Misconduct Hotline at (866) 294-9352 or www.ethicspoint.com under Texas Tech University System.

Frequency of Review

This policy will be reviewed on each even-numbered (ENY) by the Institutional Privacy Officer, and the HIPAA Privacy and Security Committee, but may be amended or terminated at any time.

Questions regarding this policy may be addressed to the Institutional Privacy Officer or the Institutional Compliance Officer.

Review Date: ~~January 3, 2022~~March 11, 2024

Revision Date: December 8, 2016, November 19, 2019, January 25, 2022, March 19, 2024