

Protect email messages from eavesdroppers!

KP's data can be most vulnerable when we are moving it from one location to another, such as via email. Encrypting our email provides security and protects our data from falling into the wrong hands.

Follow these best practices to safeguard KP's sensitive data:

- **Encrypt all emails containing PHI** that you send to a non kp.org external address by including one of the following encryption tags in the email subject line:
(phi) {phi} [phi] (PHI) {PHI} [PHI]
(encrypt) {encrypt} [encrypt] (ENCRYPT) {ENCRYPT} [ENCRYPT]
 - NOTE: the text is not case sensitive, brackets/parentheses must be included, and there must be a space between the subject and the encryption tag, e.g., Subject (PHI) instead of Subject(PHI).
 - For more information, see the TRO Send Secure Email page:
<https://cybersecurity.kp.org/how-to-send-secure-email/>
- If you are sending emails to the same recipient time after time, consider setting up **Transport Layer Security (TLS)** to automatically encrypt outgoing emails to that address. Follow this link for instructions:
[https://sites.sp.kp.org/teams/csdis/dispub/SitePages/DPS/Service%20Catalog%20Pages/SMTP%20-%20\(TLS%20Requests\).aspx](https://sites.sp.kp.org/teams/csdis/dispub/SitePages/DPS/Service%20Catalog%20Pages/SMTP%20-%20(TLS%20Requests).aspx)
- **Do not send confidential business information, PII, and/or PHI to personal email addresses, even if the email is encrypted during transmission.**
 - Sending PHI to personal email addresses allows sensitive data to be saved to non-KP devices, which is against KP policy.
 - The recipient's email domain may not be secure, putting KP data at risk.
 - If you need to access your work email at home, talk to your manager and use KP approved methods (VPN, Citrix, O365 Web Portal) to access your desktop directly, instead of forwarding messages to your personal email.

Additional email tips:

- Using **distribution lists** can cause mistakes and mis-mailings. Always verify the names on email distribution lists and double check addresses.
- Only send emails containing the **minimum necessary** amount of information to individuals who need the information to perform their job functions.
- Never send more information than is needed or requested.
 - Check all attachments for sensitive data on hidden tabs, columns, or rows, and within graphs or tables before forwarding.
 - Delete unneeded columns or tabs when sending spreadsheets.
 - Graphs and charts should be pasted as pictures into documents or PowerPoint presentations to avoid including sensitive data.
 - Saving spreadsheets and PowerPoint presentations as **PDF files** will also prevent background data from being accessible.

For more information, contact angela.b.anderson@kp.org or call her at 510-625-2413