Cautionary Tale – When Emailing PHI to a DPH colleague, be careful not to inadvertently email it to their personal email address

If you have a colleague’s personal email in your address book, it may automatically populate or default to their personal email account when you type in their name rather than their DPH email account. Recently a non-password-protected list with over 1,500 patient identifiers was sent to a number of DPH staff email accounts, one of which was the staff person’s personal email address. In addition, per policy, the email did not have SECURE in the subject line. Fortunately the email system is sometimes smart enough to detect emails that might have Protected Health Information (PHI) in them, and in this case, the email was automatically encrypted.

As a reminder, when emailing PHI:

If allowed by law to share PHI with email recipients, follow these security rules:

- **ALWAYS put “SECURE” in the subject line.** These emails will go through an encryption portal and require the recipient to reply in same safe portal.

- **DO NOT send PHI to a programmed distribution list.**

- **Double-check email addresses before you hit “reply to all.”**

- **Check to make sure there are no personal email addresses BEFORE you send.** If you create a record in Outlook with a staff member’s personal email account, we suggest you make the last name “PRIVATE Smith”. That will make a personal email easier to detect when it pops up.

- **DO NOT put patient/client names or other identifiers (eg, MRN) in the subject line.**

- **DO append this confidentiality statement in your email signature:** This e-mail is intended for the recipient only. If Protected Health Information (PHI) is contained in this email, unauthorized disclosure may subject the discloser to civil or criminal penalties under state and federal privacy laws. If you received this PHI in error, please notify me and destroy the email and any attachment immediately.