E-Mail Security

While e-mail is an important, convenient communications tool, care must be taken to maintain the confidentiality of sensitive information when using e-mail. Copies of e-mail can exist indefinitely in your, and your recipients, mailboxes, home computers, and service provider mail servers. E-mail is not secure, and efforts must be made to reduce the sensitivity of information that is shared by e-mail. If e-mail must be used to send sensitive information the following steps should be taken to reduce the likelihood of unauthorized access:

- Encrypt the e-mail and/or related attachments.
  - Note: if you have a UPHS e-mail account you can send an encrypted e-mail by typing 'encrypt' in the Subject line.
- Consider creating and encrypting a PDF to be sent, and remember not to send the decryption key in the same e-mail.
- Don’t send the e-mail to a personal account and remember that ‘Auto forwarding’ any e-mail to a non UPHS/PSOM e-mail account is not permitted.
  - Note: UPHS has disabled the forwarding of email to external addresses, other than mail.med addresses, due to security risks.
- Blind carbon copy recipients rather than listing them in the ‘To’ line when sending e-mail to multiple people. This will help to ensure the confidentiality of the recipients, e.g. patients.
- Re-check e-mail addresses and attachments before sending the e-mail. You don’t want to send the e-mail to the wrong individuals, or send the wrong information out.
- Don’t access your e-mail from an unsecured network or potentially compromised computers, i.e. Internet café, hotel computers, public Wi-Fi.

Remember, security won’t work without you. YOU are the key to security at PSOM.

Please refer all information security comments or concerns to David Wargo: David.Wargo@uphs.upenn.edu
For more security related information, visit the PMACS Information Security web page: http://www.med.upenn.edu/pmacs/