Tips & Tricks Weekly

Protect PHI Electronically

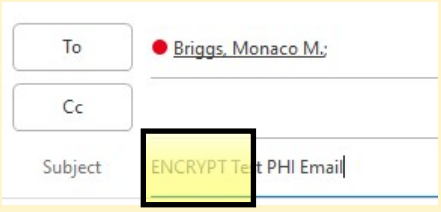
HIPAA requires healthcare organizations and their business associates to implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Technology is constantly changing and new vulnerabilities are being discovered each day. However, there are steps that each team member can take to minimize the help protect PHI.

What can you do?

1. **Delete!** Delete emails you receive that contain patient information as soon as the task associated with the email is complete. Make sure and empty your deleted items folder as well.

   If an email that contains patient information is required to be saved, save the email to your ETSU computer, password—encrypt it and delete the email.

2. **Protect!** Identify workflows in which you send large amounts (10 or more patients) of patient information via email and secure the list/report/etc. in a password-encrypted file and attach it. If your email is hacked, the hacker cannot view these password-encrypted attachments.



   A. Add the word **ENCRYPT** to the subject line. Do not include PHI in the subject line.

   B. You will password-encrypt the Word, Excel, PDF file that contains the large amount of PHI and attach it to the email. ****SEE ATTACHED WORKFLOW ON HOW TO ENCRYPT A FILE****

   C. You will share the password to the file via telephone, TigerText, or other method that does not include sending the password via email. For repetitive workflows you can establish a complex password that your team will always use for that workflow.

Remember, never remove tasks!