Tips & Tricks Weekly

Protecting PHI & Email

Chances are at some point, you have received a phishing email. **So what is phishing?** Phishing is a type of online scam where criminal send an email that appears to be from a legitimate company and ask you to provide sensitive information, such as username and password. If you click on a link in a phishing email or respond and provide your credentials, your entire ETSU email box is compromised. Because of the sensitivity of the patient information we have in our emails, and the consequence for failing to protect it, **we need every member of our team to take step to minimize the amount of patient information we maintain in our ETSU email boxes.**

What can you do?

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.

Where appropriate, copy and past emails that are clinically relevant into the patient's electronic medical record before deleting.

If an email that contains patient information is required to be kept for other documentation purposes, save the email to your ETSU computer, password-encrypt* it, and delete it from your email and deleted items folder.

*Instructions to password encrypt can be found at: https://www.etsu.edu/universitycounsel/hipaa/faq.php#answer-3-7

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.

You will still put the work encrypt in the email subject line

You will password-encrypt the Word, Excel, PDF file that contains the large amount of patient information and attach it to the email. Instructions: https://www.etsu.edu/universitycounsel/hipaa/faq.php#answer-3-7

You will share the password to the file via telephone, TigerText, or other method that does NOT include sending via email

Help Us!

Help us help others by reporting phishing email you receive. Simply forward the email to **itshelp@etsu.edu.** The phishing email will be purged from everyone's mailbox so others don't see it and click on it accidently.

If you have questions regarding patient health information and email security, please contact ETSU's HIPAA Compliance Office via email **hipaa@etsu.edu** or phone **423-439-8528**

7/8/2020