Securing Personal Devices

SECURING YOUR PERSONAL LAPTOP

- ✓ Password protect your device
  - Your password should include upper and lowercase letters, numbers, and symbols
  - Change your password at regular intervals (e.g. every 90 days)
- ✓ Install and antivirus software on your device
  - For PC: Microsoft Defender
  - For Mac: Avira
- ✓ Encrypt your device
  - For PC: Click on "Control Panel," Click on "Bitlocker Drive Encryption." Follow the instructions to turn Bitlocker on. This will encrypt your computer.
  - For Mac: Click on "System Preferences", Click on "Security & Privacy," Click on the "FileVault" tab. Follow the instruction to turn FileVault on. This will encrypt your computer.
- ✓ Secure your internet connection
  - ETSU Wi-Fi is secure
  - At home you should password protect your Wi-Fi
  - NEVER use public Wi-Fi

SECURING YOUR IPAD

- ✓ Password protect your device
  - Your password should include upper and lowercase letters, numbers, and symbols or use the fingerprint feature
  - Change your password at regular intervals (e.g. every 90 days)
    1. Click on Settings
    2. Click on Passcode
    3. Set Passcode
- ✓ Enable the auto-locking feature
    1. Click on Settings
    2. Click on General
    3. Click on auto-lock. The recommended setting is 2 minutes.
- ✓ Enable remote wiping
  - Under Settings click enable beside "Find My iPhone." Enabling this feature will allow you to login to your cloud from a computer, find your device and remote wipe the device.
- ✓ Secure your internet connection
  - ETSU Wi-Fi is secure
  - At home you should password protect your Wi-Fi
  - NEVER use public Wi-Fi

Other security related reminders:

- Do not "surf" the internet or click on links in emails while logged into the EMR
- Be diligent in identifying phishing emails

IF AT ANY TIME A DEVICE THAT CONTAINS PROTECTED HEALTH INFORMATION IS LOST OR STOLEN, PLEASE IMMEDIATELY NOTIFY THE HIPAA COMPLIANCE OFFICE ***AND ETSU*** ITS ***SO THAT WE CAN TAKE IMMEDIATE ACTION.***