Cyber Security Checklist for Personally Identifiable Information (PII)

PII is a name together with one or more of the following:
- Social security number
- Driver license number
- Financial account number in combination with any security code, access code, or password

PII Safeguards
- Do not access PII without authorization
- Access PII only using authorized applications such as my.ufl.edu
- Report exposed data immediately to UF the Privacy Office
- Unless you have special permission, do not transmit PII in email
- Never transmit PII in instant messages
- Never store PII on
  - Any computer that is not professionally managed, such as your home computer
  - A Laptop, PDA or smart phone or other portable devices
- Unless you have special permission, do not store PII on:
  - A desktop computer
    - Position screen so that it’s not viewable to others
  - Removable media such as CDs, DVDs and USB thumb drives
    - Protect media as you would a wallet or purse.
- Regardless of the use, practice the following safeguards
  - Obtain approval for all devices, media and software used with PII
  - Use strong passwords to access PII
  - Password-protected screensaver with a short time-out
  - Minimize the amount of data stored
  - Minimize the length of time data is stored
  - Encrypt stored data, preferably using whole-disk encryption
  - Only use applications that encrypt transmitted data
  - Encrypt backups and minimize backup retention time
  - Render all media unreadable prior to reuse or disposal