This SPICE EduGuide applies to HSC users of **Restricted** information on personal digital assistants (PDAs). This includes patient-identifiable information, personal identification information, and other information protected by privacy laws. Users must read and understand this document before accessing or storing **Restricted** information using a PDA. Users must maintain awareness of the exceptional risks and responsibilities of using a PDA.

Theft – PDAs are small and mobile, making them relatively easy to steal. In addition, they are expensive, highly functional and in great demand, creating high motivation to steal. Opportunity combined with high motivation makes PDAs a high risk for theft.

Disclosure of Restricted Information – Because PDAs are easily stolen or lost and because PDA data transmission is not always secure, use of PDAs present a high risk of an inappropriate disclosure of **restricted** information.

Identity Theft or Deception – A PDA ending up in the hands of an unauthorized person presents a high risk for theft of your identity or that of another person, whose personal identification information may be stored on your PDA. A great deal of damage could be done with access to personal identification information AND your email, which is easily done on an unprotected PDA.

Use safeguards for PDAs to keep **Restricted** information protected:

- You must use a PDA that has been approved by your HSC Unit Information Security Manager (http://security.health.ufl.edu/isaism/find_isa.php) and has been configured with the appropriate security. To minimize the risk of a security breach with your PDA, your HSC Unit Information Security Manager and your computer support staff will help you set up the required safeguards on your PDA, which include:
  - An engraved, indelible or electronic label with the user's name and contact information
  - A strong password
  - Encryption of data during storage and transmission
  - An inactivity log-off
  - A process to store **Restricted** and critical information on a secured server
- You must ensure that the **Restricted** information is limited to the minimum necessary to accomplish the purpose of having it stored on your PDA.
- If you are replacing or retiring your PDA, you must visit your Unit Information Security Manager for proper destruction of **restricted** information.
- If you believe your PDA has been lost or stolen, you must contact your Unit Information Security Manager immediately, so necessary steps can be taken to limit damage and liability of an inappropriate disclosure of **restricted** information.
- In general, you should treat your PDA like your wallet: keep it in a secure place when you were not carrying it, report its loss or theft, and clean it out thoroughly before discarding it.

Policy & Standards References:

GP0001 Information Classification
PS0003 Device and Media Controls
PS0006 Physical Security and Usage of End-User Computing Devices and Related Facilities
TS0003 User Account and Password Management
TS0010 Portable Computing Device Security
IR0001 Security Incident Response Team Charter