This SPICE EduGuide applies to HSC users of **Restricted** information on laptop computers. This includes patient-identifiable information, personal identification information, and other information protected by laws. Because many of the security controls in place at the HSC facilities do not follow laptop computers where users take them, users play a much more important role in the security of information they store on or access from their laptop computers. Users of laptops must maintain a heightened awareness of the security risks, recognizing that very often the responsibility rests entirely in their hands.

Theft – laptops are 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 laptops a high risk for theft.

Disclosure of Restricted Information – Because laptops are easily stolen or lost, and the ease with which **Restricted** information can be stored on them, they present a high risk of an inappropriate disclosure of **Restricted** information.

Identity Theft or Deception – A laptop 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 laptop. A great deal of damage could be done with access to personal identification information and email on an unprotected laptop.

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

- You must have authorization from your Dean, Director or Department Chair, or his/her delegate before removing Restricted information with identifiers from the UF premises on a laptop.
- You must use a laptop that has been approved by your HSC Unit Information Security Manager (find ISM, 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 laptop, your HSC Unit ISM and your computer support staff will help you set up the required safeguards on your laptop, which include:
  - A durable physical or electronic label with the user's name and contact information
  - A strong password
  - Encryption of data during storage (whole disk) and transmission (see your Unit ISM for options)
  - 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 laptop.
- If you are replacing or retiring your laptop, you must turn it in to your Unit ISM for proper destruction of any electronic **Restricted** information stored on it.
- Never leave your laptop unattended without physically locking it up, not even for a moment.
- If you believe your laptop has been lost or stolen, you must contact your Unit ISM immediately, so necessary steps can be taken to limit damage and liability of an inappropriate disclosure of **Restricted** information.

Policy & Standards References:

GP0001 Information Classification
PS0003 Device and Media Controls
TS0003 User Account and Password Management
TS0010 Portable Computing Device Security

PS0006 Physical Security and Usage of End-User Computing Devices and Related Facilities

IR0001 Security Incident Response Team Charter