

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
HEALTH INFORMATION OPERATIONAL GUIDELINES

I. Security: Personal Portable Data Devices

A. POLICY

Rev. 11/01/2006

1. **Responsibility:** All University of Florida faculty, staff, students, and volunteers are responsible for protecting all health information and personal identification information, stored on personal portable data devices, from improper use or disclosure.
2. **Devices** include, but are not limited to: Personal Data Assistants, dictation equipment, laptop or notebook computers, blackberry devices, cell phones, camera phones, digital cameras, video recorders, flash drives, and similar devices.
3. **Security of restricted information** stored in portable electronic devices is subject to the policies of the UF and HSC Information Security programs and the provisions of relevant state and federal laws.
4. **Loss or theft of portable data devices** on which restricted information is stored must be reported to the Privacy Office as well as to the University Police Department.
5. **Cameras:** Unless specifically authorized by the department chair, use of personal camera or video devices by workforce members is prohibited for work-related purposes in patient care areas, except in rare cases where the device is needed for emergency treatment of a patient.
6. **Unauthorized use or disclosure** of protected health information or personal identification information via any electronic device will be cause for disciplinary action.

B. DEFINITIONS

Personal Portable Data Device: Any easily mobile, usually hand-held, device that provides computing or information or image storage and retrieval capabilities for personal or business purposes, used by University of Florida faculty, staff, students or volunteers.

C. PRIVACY REQUIREMENTS

1. **A covered entity may not use or disclose PHI or PII** except as permitted or required by federal and state privacy regulations.
2. **Ensure the confidentiality, integrity, and availability** of all electronic PHI the covered entity creates, receives, maintains, or transmits.

D. PROCEDURES

1. **Label:** Place an engraved, electronic, or otherwise indelible label with the owner's name and contact information on all portable data devices.
2. **Protect** any PHI and PII stored on portable data devices from unauthorized access through the use of all available measures, including, but not limited to:

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
HEALTH INFORMATION OPERATIONAL GUIDELINES

- a) *Encryption,*
 - b) *Password protection,*
 - c) *Up-to-date virus protection and malicious software detection and removal products,*
 - d) *Use of data destruction procedures when information is no longer needed,*
 - e) *Use of procedures for purging, overwriting, or degaussing equipment when ownership changes,*
 - f) *Other reasonable safeguards to prevent theft of the device and/or viewing of protected health information.*
3. **Limit** protected health information and personal identification information stored on the device to the “minimum necessary”.
4. **Secure** portable data devices when not **in use by turning off and storing in a locked or otherwise secure area. Do not leave data devices in cars!**
5. **Report the loss or theft of personal data devices immediately, whether they belong to UF or not:**
- a) *To the UF Privacy Office*
 - b) *To the HSC Security Office*
 - c) *To the UF Police Department*

E. REFERENCES

HIPAA: 45 CFR §164.502 (Uses and Disclosures: General Rules), §164.312 (Technical Safeguards)

F. EXHIBITS None