

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

I. Security: General Privacy Safeguards

A. POLICY

Rev. 09/15/2005

All protected health information (PHI) and personal identification information (PII) in all formats should be secured from unauthorized access at all times, to protect the information from damage, loss, alteration, tampering, and fraudulent use.

B. DEFINITIONS

Safeguards: Rules and specific methods to protect health and identification information from unauthorized access, accidental or intentional use, disclosure, transmission, or alteration, and inadvertent or incidental disclosure to unintended recipients.

C. PRIVACY REQUIREMENTS

Safeguards: The University of Florida is required to implement appropriate administrative, technical, and physical safeguards to maintain the privacy and security of PHI & PII. (See Privacy Management: Security Standards for Electronic Records in this manual. Also see SPICE: Security Program for the Information and Computing Environment - HSC IT: <http://security.health.ufl.edu>)

D. PROCEDURES

1. Physical Safeguards

a) *Securing Paper Records*

- (1) Place paper records in protective covers that are clearly marked with the name and/or other identifier of the patient/client. Review the contents of the folder periodically to ascertain that it contains only information pertaining to that person.
- (2) Keep records and documents that are not currently in use in locations that can either be locked or that will be occupied by authorized personnel at all times. Double locking is preferred; i.e., a lockable storage unit inside a lockable room.
- (3) Keep records that are in use for treatment, payment, or health care operations purposes in the physical possession or view of an authorized workforce member at all times.
- (4) Shred discarded record documents immediately, or place them in a secure storage area for controlled shredding later. Do not place papers containing PHI / PII in open waste receptacles. Collect papers for recycling only in designated secure locations.
- (5) Place computer printers and fax machines in locations that can either be locked or that will be occupied by authorized personnel at all times.

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

b) Securing Electronic Records

- (1) To prevent unauthorized use, place computers, monitors, laptop computers, and similar data storage and display devices in areas that limit or prevent access by unauthorized persons.
- (2) To prevent unauthorized viewing of PHI / PII, position electronic data devices away from public view or shield the viewing screen.
- (3) Practitioners who access PHI / PII at home or in other non-work locations are also expected to use physical safeguards to prevent family members, roommates, and friends from unauthorized viewing of records.
- (4) Encrypt all PHI / PII stored on removable electronic storage media (discs, tapes, CD's, flash devices, etc.).
- (5) When no longer needed, physically destroy removable electronic storage media (discs, tapes, CD's, flash devices, etc.) that have been used for storing PHI or PII, or place in a locked storage unit for secure controlled destruction later.
- (6) Electronically purge data devices used to store PHI / PII before they are discarded or otherwise taken out of the control of the University.

2. Administrative Safeguards

- a) Policies and Procedures: Follow the policies and procedures for preventing, detecting, containing, and correcting information security breaches and violations, as required by Information Security personnel.*
- b) Incident Management: Report security incidents involving inappropriate use or disclosure of PHI / PII to the Privacy Office immediately.*
 - (1) Report known and suspected security incidents to the appropriate Unit Information Security Administrator and/or Manager for investigation, repair, restoration, and disciplinary action, as necessary.
 - (2) Security incidents include hoax e-mails, hacking, altered data, deliberate disruptions of service, viruses, worms, and other unauthorized use of computer accounts and systems.
- c) Notice of Termination*
 - (1) Supervisors must notify the Information Technology Department immediately when an employee terminates employment so that access to electronic data systems may be terminated.
 - (2) Supervisors are also required, when an employee terminates employment, to collect keys and other access devices if the employee's job duties included authorized access to any area where health information is stored or used.

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

3. Technical Safeguards:

a) Computer Access Controls:

- (1) To prevent unauthorized use, program all electronic data devices with log-on processes and screen-savers that turn on automatically and are password protected.
- (2) Password Controls and Guidelines
 - (a) Construct and use “strong” passwords according to UF and HSC network rules. Change passwords at least every 90 to 120 days.
 - (b) Use different passwords for different accounts, both at work and at home.
 - (c) Do not write down, post, include in e-mail, or otherwise share passwords with anyone. If the security of a password is in doubt, change it immediately.
 - (d) Do not bypass password entries by auto-logons or “remember-me” applications.
- (3) Account Management: As accounts are the means to control access, verify the identity of users, and hold users accountable.
 - (a) Create accounts only for approved requests for access that are appropriate for the system or service.
 - (b) Assign uniquely identifiable accounts to authenticated users.
 - (c) Routinely monitor accounts for use and activity.
 - (d) Authorize only those capabilities within each account that are appropriate to the user’s role requirements, responsibilities, and specific needs.

- b) Computer-Use Surveillance: The UF HSC has the capability to track and log access and activities in much of its Information and Computing Environment. All user activity on HSC Information and Computing Environment components, including, but not limited to, access through PDAs, laptops, and desktop computing devices, is subject to review.*

E. REFERENCES

1. **HIPAA:** 45CFR §164.530 (Administrative Requirements: Safeguards)
2. **UF Policies:** Acceptable Use Policy, UF Information Technology Security Policies

F. EXHIBITS: None