

Health Information Policy

POLICY

Last Rev. 07/01/2006

1. The University of Florida is committed to safeguarding the confidentiality of protected health information (PHI) to ensure that the contents of any patient records created, received, or maintained by the University of Florida are only used or disclosed in accordance with the University's policies and federal and state regulations.
2. Everyone at the University of Florida with access to PHI is responsible for safeguarding its confidentiality, and for complying with all health information privacy and security policies and procedures. This includes:
 - a. PHI in paper, electronic, video, oral, sign language or any other form.
 - b. University of Florida faculty, staff, students, volunteers, and any other persons under the direct control of the University, whether temporary or permanent, paid or not paid, also including, but not limited to, visiting and associate clinicians, faculty, students, and other persons performing services for the University.
 - c. Health information privacy and security policies and procedures approved by the University of Florida and Shands HealthCare Systems.
3. The University of Florida places significant trust in all who have access to sensitive information and with that trust comes a high level of responsibility. Uses and disclosures of patient health information for any purposes other than those described and authorized in the policies and procedures in this manual constitute confidentiality violations and are considered extremely serious. Such violations may result in immediate disciplinary action up to and including dismissal by the University of Florida.
4. Individuals formally associated with the University of Florida who access clinical records in other organizations are expected to follow that organization's requirements.

DEFINITIONS

Protected Health Information (PHI)

- a. Includes individually identifiable health information that is:
 - 1) Transmitted by electronic media or maintained in any medium defined by the federal privacy regulations as electronic media; or
 - 2) Transmitted or maintained in any other form or medium.
- b. Excludes individually identifiable health information found in:
 - 1) Education records covered by Family Education Rights and Privacy Act;
 - 2) Employment records held by a covered entity in its role as an employer.

Individually Identifiable Health Information is any health information about a patient that:

- a. Relates to the patient's past, present, or future physical or mental health, the provision of health care, or the payment for health care, **and**
- b. Identifies the patient or could reasonably be expected to identify the patient.

Confidentiality is the practice of controlling the use and disclosure of personal information so that only authorized persons or persons specifically authorized by the patient have access to such information.

Health Information Policy (continued)

PRIVACY REQUIREMENTS

1. *Limited Access:* Access to PHI in any format must be limited to those persons who have a valid business or medical need for the information, or otherwise have a right to know the information.
2. *Security:* All protected health information created, received, or maintained by the University must be secured from unauthorized access at all times, to protect the information from damage, loss, alteration, and tampering. (See also Security: Privacy Safeguards)
3. *Uses and disclosures of PHI must be limited to work-related purposes only.* Medical and financial information about patients, which becomes known to employees, volunteers, and students through authorized work-related processes, must not be used for any purpose other than the completion of assigned or approved functions.

PROCEDURES

1. *Requesting and Maintaining Access to PHI:*
 - a. Defining Levels of Access: College, department, and clinic managers define levels of access to protected health information for their workforce members, including students and other trainees, relative to assigned duties and professional "Need to Know". Access levels are based on four groups of users:
 - 1) Clinicians with orders (physicians, nurses, etc.)
 - 2) Clinicians without orders (x-ray techs, lab personnel, etc.)
 - 3) Non-clinicians with authority to transcribe orders (department secretaries)
 - 4) Non-clinicians without orders (financial and administrative personnel)
 - b. Requesting Access:
 - 1) Requests must be directed to the appropriate facility administrator, records custodian, or information systems administrator according to where the needed PHI is stored, along with the necessary documentation to justify the request.
 - 2) HSC Colleges and other UF units desiring access to electronic health information for student users should direct such requests to the Privacy Office. (See Privacy Management: Student Data Access.)
 - c. Maintaining Access:
 - 1) Managers and supervisors are responsible for the use of computers and electronic information by their workforce members, including training users, monitoring use, and discontinuing access as appropriate and required by University and Health Science Center policies.
 - 2) Individual users are responsible for ensuring their personal compliance with all the rules of use to which they agreed as a condition of gaining access to information systems.
2. *Mandatory Training for Workforce Members:*
 - a. Initial Training: **All** faculty, staff, students and volunteers, temporary and permanent, full-time and part-time, whether having access to PHI or not, who are employed by or otherwise affiliated with medical components of the University of Florida and their affiliated entities, identified as covered by HIPAA, are required, within 5 working days after hire or appointment, to:
 - 1) Complete the UF *Privacy and Security General Awareness Training*,
 - 2) Review the UF Health Information Policy, and
 - 3) Sign the UF *Confidentiality Statement*.

Health Information Policy (continued)

- b. Annual Renewal Training: All members of the workforce identified above are also required, at least once every 12 months, to complete an on-line renewal training program, and to review the Health Information Policy and re-sign the Confidentiality Statement.
 - 1) Colleges and departments may establish their own schedules for annual retraining and renewals, unless an artificial deadline must be imposed by the Privacy Office due to changes or updates in federal regulations.
 - 2) Colleges and departments are responsible for maintaining documentation showing Information Privacy training compliance by all their members.
- c. Training Responsibilities:
 - 1) Each individual, as a member of the workforce, is ultimately responsible for maintaining personal compliance with UF's Information Privacy training requirements.
 - 2) Colleges, departments, clinics, and other units are responsible for ascertaining that workforce members are in compliance with training requirements, and for maintaining documentation of compliance, as needed.
 - 3) Colleges, departments, clinics, and other units are also responsible for making all workforce members aware of Information Privacy and Security training requirements, and for incorporating appropriate training into their hiring and orientation procedures for new staff, students, and volunteers.
- 3. *Visitors and Vendors:* Any person, invited or otherwise authorized to enter University of Florida patient care areas in any location, who is not formally associated with the University shall be accompanied and/or supervised by a University Health Science Center representative at all times. The representative is responsible for the actions of the visitor.
 - a. Scope: This includes, but is not limited to, trade representatives, maintenance technicians, visiting students and health care professionals, applicants for University of Florida positions, and other similar persons or groups. This does not include family members or friends visiting or accompanying patients.
 - b. Requirements: Any of these persons who will have access or potential access to PHI during the visit shall complete the following steps *prior to beginning activities* at the University.
 - 1) Complete *HIPAA at UF: Privacy & Security for Visitors and Vendors*, using a pseudo-UF ID number, and print a certificate;
 - 2) Review the Health Information Policy and sign the *UF Confidentiality Statement*.
 - c. Visitors and students who wish to observe or "shadow" health care professionals in patient care areas must fulfill the following requirements. (See also "*Shadowing*" or *Observing Patient Care* in Section III: Privacy Management in this manual.)
 - 1) Receive sponsorship by a University Health Science Center representative;
NOTE: Visitors and students are responsible for finding, contacting, and establishing their own sponsors. The UF Health Science Centers do not provide any sponsorship services.
 - 2) Obtain permission from the appropriate college:
 - a) College of Medicine: from the Senior Associate Dean for Clinical Affairs,
 - b) All other Colleges: from the Dean of the college or designee;
 - 3) For observation within Shands Healthcare System facilities, obtain permission from the appropriate Shands Chief of Staff.

Health Information Policy (continued)

- a) Students less than 18 years old are not allowed to observe or “shadow” in patient care areas, unless they are enrolled in a UF student program.
- b) If visiting students and health care professionals will be in contact with patients during their visit, the supervising University representative must offer each patient, or the patient’s legal representative, an opportunity to agree to the presence of the visitor. Such opportunity may be offered, and agreement or objection may be received, verbally and documented in the patient’s medical record.
- d. Vendors or other company representatives who are demonstrating or supervising uses of their services or products within patient care areas of the University must:
 - 1) Check in with the appropriate clinic or department, and
 - 2) If not completed within the past 12 months,
 - a) Complete *HIPAA at UF: Privacy & Security for Visitors and Vendors* (using UF ID# 0000-0000), review the Health Information Policy, and sign the *UF Confidentiality Statement*; **or**
 - b) Provide evidence of adequate HIPAA training and a copy of the Confidentiality Statement from the vendor’s company or group.
 - 3) A Health Science Center clinic or department representative must obtain a signed Authorization for Use or Disclosure of Protected Health Information from the appropriate patient(s), authorizing the vendor to be present.
 - 4) Retain originals of all documentation in the designated college, department, or clinic administration office. Give copies of all documents to the vendor.
- 4. *Charitable Activities:* Members of the University of Florida workforce are encouraged to engage in charitable activities that benefit their communities. These guidelines have been developed to assist workforce members in making decisions about charitable activities that involve patients or clients of the UF Health Science Centers:
 - a. Protected health information or knowledge of personal affairs gained as a result of employment assignments may not be disclosed or used independently by University of Florida workforce members for charitable activities.
 - b. Members of UF’s workforce are free to make donations or participate in activities through professional charitable organizations (United Way, local Food Banks, American Red Cross, etc.), within the guidelines of those organizations and UF’s Conflict of Interest guidelines.
 - c. Charitable donations may be made to patients or clients associated with a specific program or clinic directly through that local program or clinic only with the express written approval of the program/clinic administrator and the medical director. Patients/Clients must agree to receive the charitable gifts and the activities must be documented in the individual’s medical or program record.
 - d. Activities to promote quality health care or services within the clinic or program (translation services, literacy aids, other public assistance) may be provided when and as requested by clinic/program personnel.
- 5. *Report* any known or suspected privacy or security violations involving UF’s health information to the appropriate UF Privacy Office immediately, using the Privacy Incident reporting system. (See Reporting, Investigating and Responding to Privacy Violations)
 - a. UF-Gainesville, all FGP / UFP Clinics, and all remote practice sites: UF-Gainesville Privacy Office
 - b. UF-Jacksonville and all UFJPI/ UFJHI Clinics: UF-Jacksonville Office of the General Counsel and HIPAA Compliance.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES

Health Information Policy (continued)

REFERENCES:

HIPAA Regulations: 45 CFR § 164.501 (Definitions) § 164.514(d) (Minimum Necessary Rule) § 164.530 (Administrative Requirements) (b) (Training) and (e) (Sanctions)

Florida Administrative Code (Disciplinary Action): Rules 6C1-1.008, 6C1-3.046 and 7, 6C1-4.016, and 6C1-7.048

UF Policies: Acceptable Use Policy (Information Technology), Workplace Issues: Outside Employment Policy (Human Resources), Overview: Outside Activities, Financial Interests and Conflict of Interest (UF DDD Memorandum 02/07/01)

EXHIBITS: None