SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.3. Maintaining Confidentiality of Health Information

A. POLICY

1. **Commitment:** The University of Florida (UF) is committed to safeguarding the confidentiality of protected health information (PHI) so that any patient information created, received, or maintained by UF is only used or disclosed in accordance with UF’s policies and federal and state regulations.

2. **Scope:** Every person at UF with access to PHI in any format, including without limitation, paper, electronic, graphic, video, oral/sign language, or any other format, is responsible for safeguarding its confidentiality, and for complying with all health information privacy and security policies and procedures approved by UF.

3. **Application:** UF places significant trust in all who have access to PHI and, with that trust, comes a high level of responsibility:
   a. **Uses and disclosures** of PHI for any purposes other than those described and authorized in the Information Privacy Policies and Procedures: Operational Guidelines for Health Information manual constitute privacy violations and are considered extremely serious. (This manual is available on the Privacy Office’s Health Information Privacy website.)
   b. **Violations** may result in immediate disciplinary action up to and including termination of employment and/or expulsion from academic programs by UF.
   c. **Individuals** formally associated with UF who access health records or PHI in any format in other organizations are expected to follow that organization’s requirements.

B. DEFINITIONS

1. **Confidentiality:** The practice of controlling data or information such that it is not made available or disclosed to unauthorized persons or processes.

2. **Health Information (HIPAA):** Any information, including genetic information, whether oral or recorded in any form or medium, that:
   a. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
   b. Relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient.

3. **Individually Identifiable Health Information** is a subset of health information, including demographic information collected from a patient, that relates to the past, present, or future physical or mental health of an individual, the provision of health care, or the past, present, or future payment for health care, and that identifies, or could reasonably be expected to identify, the individual.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.3. Maintaining Confidentiality of Health Information (continued)

4. **Personal Information (Florida Statutes):** An individual’s first name or first initial and last name in combination with any one or more of a defined set of data elements for that individual, or a user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account, except when such information has been encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

5. **Privacy:** The freedom of an individual from intrusion or observation; the right to maintain sole control over personal information; and the expectation that others will respect the individual’s privacy rights.

6. **Professional Need to Know:** Specific and limited information necessary to complete assigned work.

7. **Restricted Data:** Data in any format collected, developed, maintained or managed by or on behalf of the university, or within the scope of university activities, that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to, medical records, social security numbers, credit card numbers, Florida driver licenses, non-directory student records and export controlled technical data.

8. **Workforce:** UF faculty, staff, students, volunteers, and any other persons under the direct control of UF, 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 UF.

C. PRIVACY REQUIREMENTS

1. **Limited Access:** Access to PHI must be limited to those persons who have a valid business or health care need for the information, or otherwise have a right to know the information.

2. **Security:** All PHI created, received, or maintained by UF must be secured and protected at all times from unauthorized access, damage, loss, alteration, and tampering. (See also SECTION 5: Security of PHI: General Privacy Safeguards in this manual.)

3. **Limited Uses and Disclosures:** Health and financial information about patients, which becomes known to employees, volunteers, and students through authorized work- or study-related processes, must not be used for any purpose other than the completion of assigned or approved functions.

4. **Mandatory Training for Workforce Members:** All members of the healthcare workforce must be trained regarding the privacy and security policies and procedures as necessary and appropriate for them to carry out their functions.

D. PROCEDURES

1. **Access to PHI:** Address requests for access to paper or electronic records to the appropriate administrator, records custodian, or information systems coordinator according to where the PHI is stored. Provide required documentation as necessary to justify the request. (See SECTION 5: Security of PHI: Security Safeguards in this manual.)
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.3. Maintaining Confidentiality of Health Information (continued)

2. **Mandatory training for all UF workforce members:** At orientation and annually, complete an appropriate UF training module, review the UF Health Information Policy and sign the UF Confidentiality Agreement. (See **SECTION 1: Education and Training** in this manual for detailed requirements.)

3. **Health Care Volunteers:** Register through Human Resources Services in the college where the volunteer will be working or where the volunteer’s sponsor is employed. Volunteer activities that involve access to PHI (active or passive) must be approved by the UF Privacy Office. Volunteers follow the same privacy training requirements as HSC employees. (See **SECTION 6: Other Procedures – Volunteering and Observing** in this manual.)

4. **Visitors and Vendors:** Any person, invited or otherwise authorized to enter UF patient-care areas, but not formally associated with UF’s Health Science Center or Student Health Care Center, must be accompanied and/or supervised by a UF representative at all times. The representative is responsible for the actions of the visitor.

5. **Charitable and Other Outside Activities:** Members of the UF workforce are encouraged to engage in charitable and other activities that benefit their communities:
   
a. PHI or knowledge of the personal affairs of patients or clients that has been gained as a result of job, volunteer, or student assignments may not be disclosed or used independently by UF workforce members for charitable or other outside activities.

b. **UF workforce members** are free to participate in or make donations to 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 must agree to receive the charitable gifts, and the activities must be documented in the individual’s health or program record.

d. **Activities** to promote quality health care or services within a clinic or program (translation services, literacy aids, or other public assistance) may be provided when and as requested by clinic/program personnel.

6. **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 **SECTION 1: Reporting and Responding to HIPAA Privacy Violations** in this manual.)

E. REFERENCES

1. **HIPAA Regulations:** 45 CFR §160.103 – Definitions; § 164.308 – Administrative safeguards: (a)(3) Workforce Security, (a)(4) Information Access Management, (b) Training; (e) Sanctions

2. **Florida Statutes:** 501.171(g) (Security of confidential personal information)
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.3. Maintaining Confidentiality of Health Information (continued)


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

F. EXHIBITS

1. Website: Confidentiality Statement

2. See also Privacy Forms: Confidentiality Statement