Table of Contents

SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.1. Relationship of University of Florida Components and Entities Explained
   University of Florida Health Care Components
   Affiliated Entities
   Developing and Maintaining Procedures

1.2. Protected Health Information and De-Identification
   The 18 HIPAA-defined Identifiers
   De-Identification and Re-identification of PHI
   PHI of Deceased Individuals

1.3. Maintaining Confidentiality of Health Information
   UF’s Commitment to Privacy & Confidentiality
   Privacy Policies: Scope and Application
   Access to PHI
   Mandatory Training
   Healthcare Volunteers, Visitors and Vendors
   Charitable and Other Outside Activities

1.4. Reporting and Responding to Violations Involving PHI
   Reporting Privacy Violations
   Investigations and Disciplinary Actions
   Required Notifications for Privacy Breaches
   Mitigation
   Required Notification for Breaches of PHI
   Disclosures by Whistleblowers and Non-Retaliation
   Preventing, Responding to, and Reporting Incidents
   Additional Procedures for Managers
   - Responding to Complaints
   - Responding to Loss or Inappropriate Disclosures of Information

1.5. Verification of Identity and Authority and Personal Representatives
   Verification Requirements
   Evidences of Identity
   Personal Representatives
   Exercise of Professional Judgment
   Minors, Incapacitated Adults, Deceased Individuals
   Verifying the Authority of Public Officials

1.6. Minimum Necessary Rule
   Limiting Uses, Disclosures and Requests
   Table: Minimum Necessary Decision Tree
   Table: Examples of Routine & Non-Routine Disclosures/Requests
Table of Contents (continued)

1.7. Education and Training 38
   Training Requirements
   Documentation of Training
   Personal and Departmental Responsibilities for Training
   Training Programs
   - Level 1: General Awareness / HIPAA for Researchers
   - Level 2: Policies and Procedures
   - Level 3: Role-Specific

SECTION 2: HEALTH INFORMATION AND RECORD MANAGEMENT

2.1. Health Information Management: General Policies 43
   Maintenance and Ownership of UF Records
   Confidentiality and Availability of Records
   Content of UF Health Records
   Use and Disclosure of Health Information
   Removal of Patient Information from UF Health Premises
   Health Information Custodians at UF
   Health Information Management Personnel
   - Table: Designated Record Set 47
   - Table: Medical Record Custodians List 48

2.2. Health Information Management: Documentation Rules 49
   Authorization to Document
   General Documentation Requirements: Paper / Electronic Records
   Additions/Amendments/Corrections
   Copies of Health Records from Other Facilities/Providers
   Record Errors That Cannot Be Corrected by the User
   Co-Signatures

2.3. Health Information Management: Record Management Guidelines 52
   Storage, Security, and Control of Active Records
   Removal of Health Information from Premises
   Duplication of Patient Information
   Recovery of Lost or Damaged Paper Records
   Management and Organization of Paper Records
   Record Management during Disasters
   When Record Recovery Is Not Possible
Table of Contents (continued)

2.4. Health Information Management: Retention, Archiving, and Disposal 57
   - Retention Rules for Records
   - Archiving and Storing Inactive Records
   - Disposal and Destruction of Records
   - Preparing Records for Storage; Retrieving Records
   - Disposing of Non-Primary Record Documents Containing PHI
   - Permanently Destroying Whole Health Records
      *Table: Appropriate Record Destruction Methods* 62

SECTION 3: USES AND DISCLOSURES OF PHI

3.1. Uses and Disclosures of PHI: General Rules 63
   - General Rules for Uses and Disclosures of PHI
   - Information Subject to More Stringent Laws
   - UF’s Organized Health Care Arrangement
   - Disclosing PHI to Other Entities
   - Uses and Disclosures of PHI Permitted Without Patient Authorization
   - Other Limited Uses and Disclosures of PHI Permitted
      *Procedures:* 66
         - General Rules for Providing Copies of Records
         - Documenting and Maintaining a Log of Disclosures of PHI
         - Purchasing/Updating Products or Systems That Use Electronic PHI
         - Responding to Agencies Claiming Exemption from HIPAA
         - Responding to Media Requests for Patient Information

3.2. Uses and Disclosures of PHI: “Super-Confidential” Health Information 69
   - Information Specifically Protected by Law
   - Limited Disclosures
   - Responding to requests for Super-Confidential Health Records
      - By Patient Authorization
      - By Subpoena or Court Order
   - Required Non-Redisclosure Statements

3.3. Uses and Disclosures of PHI: Family Members and Friends 74
   - Scope, Application, and Expectations
   - Patients’ Rights to Restrict Disclosures
   - Definition of “Family Member” and “Personal Representative”
   - Verification of Identity and Authority
   - Written and Verbal Authorizations
Table of Contents (continued)

3.4. Uses and Disclosures of PHI: Authorizations for Release of Health Information 78
   Uses and disclosures of PHI must be authorized
   Verification Required
   Valid Authorizations
   Revoking an Authorization
   Use of Authorization Forms
   Expiration Dates
   Alteration or modification of Authorization forms
   Retention of Authorization Forms
   Verbal Agreements/Authorizations

3.5. Uses and Disclosures of PHI: Health Records for Depositions 81
   Using and Disclosing Health Records for Depositions
   Notifying the Deposing Attorney

3.6. Uses and Disclosures of PHI: Subpoenas, Court Orders, and Attorney Requests 83
   Providers Who Receive a Subpoena
   Processing Requests for Health Records for Judicial Purposes
   Certifying Copies of Records
   Table: Copying, Production, and Inspection Fees 85

3.7. Uses and Disclosures of PHI: Fundraising 86
   Rules for Using PHI in Fundraising
   Privacy Office Approval Required
   Written Authorization Required
   Opting Out and Maintaining the Opt-Out Log
   Institutionally-related foundations involved in fundraising

3.8. Uses and Disclosures of PHI: Marketing 89
   Rules for Using PHI for Marketing
   Written Authorization Required
   Maintaining the Opt-Out Log
   Sale of PHI Prohibited
   Direct / Indirect Remuneration

3.9. Uses and Disclosures of PHI: Research 92
   Authorization Required
   De-Identified Health Information
   Honest Broker Services
   Requesting Health Records, Information and Data for Research
   Using Compound Authorizations
   Document Retention and Storage
   Research on Three or Fewer Subjects / Case Studies
   Correcting Improper Procedures: 30-Day Cure
   - Failure to Obtain Authorization
   - Failure to Obtain Waiver of Authorization
Table of Contents (continued)

3.10. Uses and Disclosures of PHI: Sale of PHI
   Authorization Required for Sale
   Sale of PHI Exclusions

SECTION 4: PATIENT’S RIGHTS

4.1. Patient’s Rights: The Notice of Privacy Practices
   Notice and Acknowledgement of Receipt Required
   Availability of the Notice
   Changes in the Notice
   Organized Health Care Arrangement

4.2. Patient’s Rights: Access to Personal Health Records
   Right to Inspect or Receive Copies
   When the Right of Access Does Not Apply
   Authorizations
   Health Records of Deceased Patients
   To Receive Copies of Records
   To Inspect or View Records
   Table: Copying and Inspection Fees

4.3. Patient’s Rights: Request to Restrict Uses and Disclosures of PHI
   Requests for Restrictions
   Certain Requests for Restrictions Require Compliance
   Decisions to Grant or Deny Requests
   Changes or Additions in Requests for Restrictions
   Terminating the Restriction
   Coordinating, Documenting, and Communicating the Response Decision

4.4. Patient’s Rights: Request for More Confidential Communications
   Verbal and Written Communications
   Final Decision-Making Authority
   Procedures
   - Verification
   - Response Coordination

4.5. Patient’s Rights: Amendment of Records
   Responding to Requests for Amendments
   Privacy Office Review
   Procedures for Managers
   Privacy Office Involvement
   Making Amendments
   Documenting the Response
   Future Disclosures
   Amendments from Other Providers
Table of Contents (continued)

4.6. Patient’s Rights: Privacy Complaints  
Right to File a Complaint  
Non-Retaliation and No Waiver of Rights  
Where to File Complaints/Addresses  
Informing the Privacy Office of Complaints and Follow Up

4.7. Patient’s Rights: Accounting for Disclosures  
Background for Understanding the Requirement  
Patient’s Right to Request an Accounting  
\textit{Time limitations, Report format, and Fees}  
Using the Online DTS  
Requesting an Accounting of Disclosures  
Responding to Written Requests for Accounting of Disclosures  
Temporary Suspension of Right to Receive an Accounting  
Accounting for Disclosures during Research

SECTION 5: SECURITY OF PHI

5.1. Security of PHI: Privacy Safeguards  
Computer Surveillance  
Physical Safeguards: Securing Paper and Electronic Records  
Administrative Safeguards  
\textit{Policies and Procedures}  
\textit{Incident Management}  
\textit{Notice of Termination}  
\textit{Required Training}  
Technical Safeguards  
\textit{Computer Access Controls}  
\textit{Acquiring, Maintaining, and Terminating Access to PHI}

5.2. Security of PHI: Personal Portable Data Devices/ Mobile Devices  
Devices Included  
Security and Loss or Theft of Devices  
Use of Personal Devices and Cameras  
\textit{Examples of Acceptable and Unacceptable Uses}  
User Permissions for Communicating PHI  
User Protocols and Etiquette  
Training  
Protecting Personal Devices and Contents  
Limiting Users and Data  
Securing Devices When Not In Use  
Disposing of Devices  
Reporting Loss or Theft
### Table of Contents (continued)

#### 5.3. Security of PHI: Electronic Databases
- Requirements for Securing Databases
- Products of Electronic Databases
- Transport of Data
- Purging and Destruction of Data

#### 5.4. Security of PHI: Electronic Mail
- Application and Scope
- Conditions for Including PHI in E-mails
  - Patients and Research Participants
  - Staff-to-Staff
  - Internal E-mails
  - Research Communications
  - External E-mails
- Patient Communications via EHR System
- Alerting Patients of E-mail Hazards
- E-mail Disclaimer Notice

#### 5.5. Security of PHI: Video- and Audio-Conferences
- Pre-Approval Required
- Conference Elements to Be Approved
- Patient Rights
- Personal Communications Not Included

#### 5.6. Security of PHI: Verbal, Telephone, and Other Types of Communications
- Use of Interpreters
- Use of Telephone Devices for the Hearing Impaired
- Verbal and Substitute Communications in Healthcare
- Telephone Use in Healthcare Areas

#### 5.7. Security of PHI: Faxing Protected Health Information
- Fax Cover Sheets
- Confidentiality Disclaimer
- Pre-programming Fax Numbers
- Verification Procedures
- Reporting Faxing Errors
**Table of Contents (continued)**

**SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES**

6.1. **Visitors, Vendors, Volunteers, and Observers**  
General Rules  
*Exception for Visiting Faculty*  
*Observing and Volunteering by Minors*  
*Sponsor Responsibilities*  
*Patient Authorizations for Observer’s Presence*  
*Access to PHI and Restricted Data*  
*Required Training*  
Privacy Policies for Volunteering  
Privacy Policies for Observing or “Shadowing”  
*Individual Observers*  
*Groups of Observers*

6.2. **Student Data Access – Electronic Medical Records**  
Pre-Approval Required for UF Students  
Programs Authorized for Access to PHI  
Students who are also employees  
Sponsors and Their Responsibilities  
Student Responsibilities  
Time Limits and Standards for Access  
Shands Requirements  
Non-Compliance  
Use of Data  
Access to PHI for Research  
Procedure for requesting and acquiring access for students

6.3. **Honest Broker Certification**  
Uses and Disclosures of PHI for Research  
Honest Broker Requirements  
*Sponsorship or Appointment*  
*Education and Training*  
*Application Process*  
*Attestation of Agreement*  
Procedures:  
*Certiﬁcation, Approval and Maintenance*  
*Adding and Removing Brokers*  
*Duties and Other Requirements*  
*Honest Broker Data Requests*  
*Non-Compliance*
NOTICE: All policies in the following pages apply to all of the following entities: The University of Florida Health Science Centers, together including the UF Health Science Center clinics and physicians’ offices; the University of Florida Student Health Center, the University of Florida Wellness and Counseling Center; the University of Florida Colleges of Medicine, Nursing, Health Professions, Dentistry and Pharmacy; the Florida Clinical Practice Association; the University of Florida Jacksonville Physicians, Inc.; the University of Florida Jacksonville Healthcare, Inc.; and other affiliated health care providers, including all faculty, employees, students and volunteers.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.1. Relationship of University of Florida Components and Entities Explained

A. POLICY

1. Designations: The following health care components and affiliated entities have been designated as parts of one common entity at the University of Florida (UF) for purposes of complying with the federal privacy regulations found at 45 CFR Parts 160 - 164, commonly referred to as HIPAA:

   a. University of Florida Health Care Components:
      1) The University of Florida Health Science Center (with locations in Gainesville and Jacksonville), together including:
         a) UF medical, dental, and nursing clinics and physicians’ offices, including those entities commonly referred to as University of Florida Physicians (UFP);
         b) UF Colleges of Medicine, Nursing, Health Professions, Dentistry and Pharmacy;
         c) UF College of Veterinary Medicine, in limited circumstances;
      2) UF Student Health Center,
      3) UF Speech and Hearing Clinic,
      4) The McKnight Brain Institute,
      5) IFAS Dietetics Intern Program,
      6) The Wellness Center’s Cardiac Rehab Program
      7) UF Counseling and Wellness Center

   b. Affiliated Entities
      1) All direct support organizations and health service support organizations for the various Health Science Center components, including, but not limited to:
         a) Florida Clinical Practice Association, Inc.,
         b) UF Jacksonville Physicians, Inc.;
         c) Faculty Associates, Inc.
         d) Florida Health Professions Association, Inc.
         e) UF College of Nursing Faculty Practice Association, Inc.
         f) UF College of Pharmacy Faculty Practice Association, Inc.
         g) UF Jacksonville Healthcare, Inc.;
      2) The UF Research Foundation, Inc.
      3) The Florida Proton Therapy Institute
      4) The Institutional Review Boards 01, 03 and 04
      5) Other health care providers, health care plans or health care clearinghouses that have been or may be designated as affiliated entities for purposes of compliance with the Privacy Rule.

2. Application: Solely for purposes of compliance with the Privacy Rule, these components or entities will be treated as one common entity. (See HIPAA Organizational Requirements: Hybrid Entity in the HIPAA Privacy Management manual for further explanation of hybrid entity status and affiliated covered entity status, and associated requirements.)
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.1. Relationship of UF Components and Entities Explained (continued)

3. **Scope:** As a result of the decision to utilize permitted designations to pursue compliance with the federal Privacy Rule by the components and entities named above, the Privacy of Health Information policies, procedures, and operational guidelines developed and approved by the University of Florida shall apply to all the above named entities equally, to the extent that they apply to the functions of that component or entity.

**B. DEFINITIONS**

1. **Affiliated Covered Entity:** Legally separate covered entities that are associated in business.

2. **Common control** exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

3. **Common ownership** exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

4. **Covered Entity:** a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by the Privacy Rule.

5. **Hybrid Entity:** A single legal entity that is a covered entity, whose business activities include both covered and non-covered functions, and that designates health care components in accordance with the Privacy Rule.

**C. PRIVACY REQUIREMENTS**

1. **Legally separate covered entities** that are affiliated may designate themselves as a single covered entity for purposes of the privacy regulations.

2. **Health Care Components:** The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation.

3. **Policies and Procedures:** A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of the privacy regulations.

**D. PROCEDURE**

1. **Application:** Any of the components or entities named above shall simply substitute its own name for “the University of Florida” wherever found throughout this manual.

2. **Specific Procedures:** Entities and components should develop and incorporate appropriate additional procedures (within the confines of the policies and guidelines) that correspond to the particular needs and functions of the entity to assure compliance with the privacy regulations. The Chief Privacy Officer must approve these additional guidelines before they become effective.

3. **Updates:** All entities and components named above are responsible for updating entity-specific procedures as needed to comply with changes in the law.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.1. Relationship of UF Components and Entities Explained (continued)

E. REFERENCES:

1. HIPAA Regulations: 45 CFR §164.530(i) Administrative requirements: Policies and procedures; §164.504(a-d) Uses and disclosures: organizational requirements

2. Board of Governors’ Regulations: 9.017, 9.011

F. EXHIBITS:

None
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.2. Protected Health Information and De-identification

A. POLICY

1. **Specification:** The University of Florida (UF) will use the definition of Protected Health Information (PHI) as specified in the Privacy Rule, also known as HIPAA.

2. **De-identification:** UF may determine that health information is not individually identifiable health information by applying the criteria for de-identification outlined in the Privacy Rule. Health information that does not identify an individual, and for which there is no reasonable basis to believe that the information can be used to identify an individual, is not subject to the Privacy Rule.

3. **Re-identification:** A code or other means of record identification may be assigned to allow information to be re-identified, within the guidelines of the Privacy Rule.

4. **Deceased Individuals:** If decedent health information is maintained for longer than 50 years following the date of death of the individual, this information will no longer be subject to the Privacy Rule.

B. DEFINITIONS

1. **De-Identified Health Information:** Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

2. **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.

3. **Protected Health Information (PHI),** as defined by HIPAA:
   
a. Individually identifiable health information transmitted by or maintained in electronic media, or in any other form or medium.

   b. **PHI excludes** individually identifiable health information found:
      1) in Education records covered by the Family Education Rights and Privacy Act (FERPA);
      2) in Employment records held by a covered entity in its role as an employer.
      3) Regarding a person who has been deceased for more than 50 years.

   **Note:** The 50-year period of protection for decedent health information under the Privacy Rule does not override or interfere with UF’s retention policies, State or other laws that provide greater protection (even after 50 years) for “super-confidential” information, or the professional responsibilities of mental health or other providers.

4. **Re-identification:** The process of making health information that has previously been deidentified capable of identifying an individual again.
C. PRIVACY REQUIREMENTS

1. De-identification of protected health information: Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information. A covered entity may determine that health information is not individually identifiable health information only if:

a. **Statistical Method:** A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

   1) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

   2) Documents the methods and results of the analysis that justify such determination; or

b. **“Safe Harbor” Method:**

   1) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

   a) Names;

   b) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

      i. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

      ii. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

   c) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

   d) Numbers, including: Telephone numbers; Fax numbers; Social security numbers; Medical record numbers; Health plan beneficiary numbers; Account numbers; Certificate/license numbers; Vehicle identifiers and serial numbers, including license plate numbers; Device identifiers and serial numbers;

   e) E-mail and Internet information, including: Electronic mail addresses; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers;

   f) Biometric identifiers, including finger and voice prints;

   g) Full face photographic images and any comparable images; and
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.2. Protected Health Information and De-identification (continued)

h) Any other unique identifying number, characteristic, or code, except as permitted under
   Re-identification below; and

2) The covered entity does not have actual knowledge that the information could be used alone or
   in combination with other information to identify an individual who is a subject of the
   information.

2. **Re-identification:** A covered entity may assign a code or other means of record identification to allow
   information de-identified under this section to be re-identified by the covered entity, provided that:
   a. **Derivation:** The code or other means of record identification is not derived from or related to
      information about the individual and is not otherwise capable of being translated so as to identify
      the individual; and
   b. **Security:** The covered entity does not use or disclose the code or other means of record
      identification for any other purpose, and does not disclose the mechanism for reidentification.

3. **Deceased individuals:** A covered entity must comply with the General Rules for uses and disclosures of
   PHI for a period of 50 years following the death of the individual.

D. PROCEDURES

1. For assistance in determining if health information qualifies as PHI or if PHI has been properly de-
   identified, call the Privacy Office.

2. To de-identify or re-identify health information: apply one or more of the criteria/processes listed in
   the Privacy Requirements above.

3. **Retention of records for deceased individuals:** Follow UF’s record retention schedule (see SECTION 2:
   Health Information Management: Retention, Archiving and Disposal) unless retention of specific
   records is warranted for a longer period of time. Do not maintain health records longer than necessary.

E. REFERENCES

HIPAA: 45 CFR §160.103 Definitions; §164.502 Uses and Disclosures: General Rules (f) Deceased
   Individuals; §164.514(a) De-identification of Protected Health Information; §164.514(c) Re-
   identification

F. EXHIBITS

None

[Back to Table of Contents]
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 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 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**

Confidentiality Statement

Back to Table of Contents
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.4. Reporting and Responding to Violations involving Protected Health Information

A. POLICY

1. **Expectations**: The University of Florida (UF) promotes ethical standards of conduct and encourages all members of its workforce and the workforce of its affiliated entities to honor the privacy rights of patients, clients, students, employees, and volunteers.

2. **Reporting**: All unauthorized uses, disclosures, or acquisitions of protected health information (PHI) or other restricted data, known and suspected, must be reported to the appropriate UF Privacy Office in Gainesville or Jacksonville immediately.
   
   a. **All UF workforce members**, especially those who are employed by or otherwise associated with UF’s healthcare components and affiliated entities, are obligated to report any known or suspected violations, including breaches or unauthorized uses, disclosures or acquisitions of PHI or other restricted data immediately upon discovery.
   
   b. **Reporting forms and telephone numbers** are posted on the UF Privacy Office website: [http://privacy.health.ufl.edu](http://privacy.health.ufl.edu). Telephone numbers are also in the UF Health Notice of Privacy Practices.

3. **All complaints and reported violations** of information privacy and security will be investigated according to the General Privacy Management policy: *Investigating and Responding to Privacy Violations*. If violations of privacy are confirmed, the Privacy Office will recommend corrective actions and sanctions, notify or assist with notifying affected individuals as appropriate, and try to mitigate, to the extent possible, any harmful effect of a confirmed privacy violation.

4. **Non-Retaliation and Whistleblowers**. See Privacy Requirements below.

5. **Investigations and Disciplinary Action**: The Chief Privacy Officer (CPO) or a designee appointed by the CPO is responsible for investigating and/or assisting with investigations of all suspected violations involving PHI or other restricted data created and maintained by UF and its affiliated entities. (See *Investigating and Responding to Privacy Violations* and its corresponding flowcharts in the General Privacy Management manual for procedural details.)
   
   a. **Members of UF’s workforce** who fail to comply with UF’s privacy policies and procedures or with the requirements of the state and federal privacy regulations will be disciplined in accordance with UF’s normal disciplinary procedures, up to and including termination of employment and/or expulsion from UF.
   
   b. **Members of UF’s affiliated entities** who fail to comply with applicable UF privacy policies and procedures or with the requirements of the state and federal privacy regulations will be disciplined in accordance with those entities’ normal disciplinary procedures, up to and including termination of employment.

6. **Mitigation**: UF will make good faith efforts, as required by the Privacy Rule, to mitigate, to the extent practicable, any harmful effect that is known to have occurred as a result of a use or disclosure of PHI by UF or its business associates in violation of UF’s policies and procedures or of the privacy regulations.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.4. Reporting and Responding to Violations (continued)

a. The following factors will be evaluated to determine the best mitigation strategies:
   1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   2) The unauthorized person who used the PHI or to whom the disclosure was made;
   3) Whether the PHI was actually acquired or viewed; and
   4) The extent to which the risk to the PHI has been mitigated.

b. After investigation, if mitigation is required, departments and/or individuals involved in the privacy breach may be asked to assist in mitigating harmful effects.

7. Required Notification for Breaches of PHI and/or Other Restricted Data:

a. UF is required by both federal and state laws, following the discovery of a breach of unsecured PHI or other restricted data, to notify specified government agencies and/or each individual whose information has been, or is reasonably believed to have been affected by such a breach, according to the definitions of those laws. Any exceptions must be approved by the Chief Privacy Officer.

b. The UF-Gainesville Privacy Office will oversee all aspects of the notification process; the College, Department, Division, or other UF unit from which the unsecured PHI was acquired will be responsible for the costs and labor associated with notifying the affected persons.

c. UF will notify the Department of Health and Human Services of any breaches of unsecured PHI, as required by and using the terms as defined by the HIPAA regulations. UF will also notify the Florida Department of Health of any breaches of security, as required by and using the terms as defined by the Florida Statutes.

B. DEFINITIONS

1. Incident: An event, whether electronic, physical or social that adversely impacts the confidentiality, integrity or availability of University of Florida data or information systems; or a real or suspected action, inconsistent with University of Florida Privacy or Acceptable Use policies.

2. Mitigation: To make less severe, to partially remove, or to correct, so that harmful effects of a privacy violation are reduced or eliminated.

3. Unsecured Protected Health Information (HIPAA): PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services; specifically, encryption for electronic PHI, and destruction for all other PHI.

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.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.4. Reporting and Responding to Violations (continued)

5. **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.

6. **Uses and Disclosures:**
   a. **Accidental Uses and Disclosures:** Unintentional uses and/or disclosures of PHI or other restricted data that occur as a result of human error or circumstances beyond the control of the individual, even when established policies and procedures were followed. Accidental uses and/or disclosures of PHI are Privacy Incidents and must be reported.
   b. **Incidental Disclosures:** Unintentional disclosures of PHI or other restricted data occurring during the normal course of business, which are incidental to an otherwise permitted use or disclosure of the information. If a workforce member is taking reasonable precautions, and another individual happens to see or overhear private data that the workforce member is using, the workforce member will not be held liable for that disclosure and usually does not need to report it as an incident.
   c. **Intentional Uses and Disclosures:** Uses and disclosures of PHI or other restricted data that occur as a result of careless, deliberate, and/or pre-meditated disregard of established policies and procedures, with or without malicious intent. Intentional uses and disclosures are Privacy Incidents that will result in disciplinary action and the application of sanctions by UF. They may also result in personal liability, either in civil or criminal legal action.

7. **Violation:** Infraction of a law; going against established rules.

C. PRIVACY REQUIREMENTS

1. **Notification:** A covered entity shall, following the discovery of a breach of unsecured PHI or other restricted data, notify each individual whose information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

2. **Sanctions:** A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of the Privacy Rule. A covered entity or business associate must apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

3. **Disclosures by whistleblowers:** A covered entity is not considered to have violated the HIPAA requirements if a member of its workforce or a business associate discloses PHI, provided that:
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.4. Reporting and Responding to Violations (continued)

   a. The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

   b. The disclosure is to:

      1) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

      2) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described above.

4. Refraining from intimidating or retaliatory acts: A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

   a. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by the Privacy Rule, including the filing of a complaint under this section;

   b. Any individual or other person for:

      1) Filing of a complaint with the Secretary under the HIPAA regulations;

      2) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under the HIPAA regulations; or

      3) Opposing any act or practice made unlawful by the HIPAA regulations, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA.

5. Mitigation: A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

6. Policies and Procedures: A covered entity must implement policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, or other requirements of the Privacy Rule.

D. PROCEDURES

1. Preventing Privacy Incidents:

   a. Take reasonable precautions to avoid incidental disclosures:

      1) Speak in a low, soft voice while discussing private information;

      2) Move to as private a location as possible while using private information;
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.4. Reporting and Responding to Violations (continued)

3) Keep private data in all formats secured from persons who do not have authorization or a legitimate need to know the information.

b. Employ measures to prevent accidental or intentional uses and disclosures of PHI:
   1) Know and follow UF’s policies and procedures concerning proper handling of PHI.
   2) Pay attention to details when using or disclosing PHI: for example, double-check e-mail addresses and messages, and look at all pages of paper copies of PHI before delivering them.
   3) Remain aware at all times of the confidential nature of PHI and of the environment in which the information is being used, disclosed, or requested. (See “Take reasonable precautions…” above.)

2. First Response to Incidents: If an unauthorized (accidental or intentional) use, disclosure or acquisition of PHI or restricted data occurs, or is suspected to have occurred:
   a. Step in to correct the situation, if possible and appropriate. For example: interrupt an improper conversation in an elevator; rescue a document left in a public place; or lock an unlocked area that allows access to private data.
   b. If the breach involves a computer system containing private data:
      1) Take immediate steps to secure the affected system. Follow UF and departmental information security procedures.
      2) Report the breach, along with your contact information, immediately to your supervisor, your unit’s Information Security Manager, and the appropriate UF Privacy Office (Gainesville or Jacksonville).
      3) If a computer or other data management device has been lost or stolen, also notify the University Police Department, the Jacksonville Sheriff’s Office, or your local law enforcement agency, as appropriate.

3. When to Report a Privacy Incident, Known or Suspected:
   a. Incidental disclosures of PHI are not considered Privacy Incidents and do not usually need to be reported. However, members of the workforce should use professional judgment to assess the potential outcome(s) of an incidental disclosure and report any that may result in a fraudulent or criminal misuse of the information or have a negative impact on UF or its affiliated entities.
   b. Accidental and intentional uses and disclosures of PHI must be reported immediately.

4. How to Report a Privacy Incident:
   a. Complete a Privacy Incident Report (see Forms) immediately, if possible, but no later than the end of your shift or workday. Two forms are available: one for PHI and one for Private Data (not PHI).
      1) Include the following information:
         a) Date, time and location of the incident:
            i. Include the date of the report as well as the date of the incident;
            ii. Time may be estimated or omitted, if not known;
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.4. Reporting and Responding to Violations (continued)

iii. Location should be the College, Department, Division, Clinic or other Unit responsible for or where the incident originated.

b) The nature of the violation: What happened? Provide a clear, specific, detailed description including what, where, how, and why, if available.

c) Type of private data involved: Paper records, electronic records, or other type of data.

d) Other persons involved: Names, titles, contact information, and how they were involved.

2) Any immediate harm known or observed: Was control of the PHI or restricted data lost? Was PHI or restricted data misused, disclosed, altered, damaged, or destroyed? Did an affected individual or other person voice concerns or file a complaint?

3) Patient Awareness: Indicate whether the patient (or legal representative) is aware of the disclosure or not. If the individual is unaware of the incident, the Privacy Office will either inform them or instruct the responsible unit to do so.

4) Immediate corrective actions already taken: for example, documents or computers were secured, recipient of PHI was asked to return or destroy the data, misdirected e-mail was retracted, misdirected documents were returned, etc.

b. Send the Privacy Incident Report to the Privacy Office immediately.

1) For all UF-Gainesville faculty practice clinics, all HSC and health-related colleges and departments, all remote practice sites (except Jacksonville sites), and the Student Health Care Center: report to the UF-Gainesville Privacy Office.

2) For All UF-Jacksonville HSC colleges, departments and clinics, and all UFJPI/ UFJHI Clinics: report to the UF-Jacksonville Privacy Manager.

E. ADDITIONAL PROCEDURES FOR MANAGERS


2. Responding to Loss or Inappropriate Disclosure of Information
   a. Misplaced or Stolen Paper Records: (For record-recovery/replacement procedures, see SECTION 2: Health Information Management: Record Management Guidelines in this manual.)
      1) If every effort has been made to retrieve a lost paper record and it has been determined that retrieval is unlikely, log the loss into the Disclosure Tracking System as an accidental disclosure.
      2) If a paper record that was believed to be lost or stolen is later recovered, notify the Privacy Office; do not attempt to alter the entry in the Disclosure Tracking System.
   
   b. Inappropriate Disclosures: If PHI or other restricted data is e-mailed, mailed, faxed, or otherwise delivered to an incorrect address or the wrong individual:
      1) Report all instances of misdirected information on an Incident Report to the Privacy Office as soon as they are discovered.
      a) It is better to wait for instructions from the Privacy Office before notifying the affected patient.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.4. Reporting and Responding to Violations (continued)

b) If the recipient reports the erroneous delivery, document the conversation and/or include any written communications from the recipient with the Incident Report.

2) Make every effort to retrieve the information that was sent (have it mailed back or hand-carried), or get assurance, preferably in writing, from the recipient that it was destroyed or deleted.
   a) Document these efforts and the results on the Incident Report form.
   b) Document any verbal assurances from the recipient that the information was destroyed or deleted.

3) Log the disclosure into the Disclosure Tracking System, if instructed to do so.

F. REFERENCES:

1. HIPAA Regulations: 45 CFR §164.308 Administrative safeguards; §164.400 - 164.414 - Notification in the Case of Breach of Unsecured Protected Health Information; §164.502 (j) Whistleblowers; §164.530 (e) Sanctions; (f) Mitigation; (g) Non-retaliation; (i) Policies and Procedures;

2. Florida Statutes: 112.3187, Florida's Whistle-blower's Act; 817.568, Criminal use of personal information; 501.171, Security of confidential personal information

3. University Rules: Rules UF-1.008(1)(o), UF-3.047(3)(d), UF-4.016(2)(o) and (t), and UF-7.048(1)(c)

G. EXHIBITS:


Back to Table of Contents
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.5. Verification of Identity and Authority and Personal Representatives

A. POLICY

1. Verification Required: Prior to any disclosure, restriction, amendment, or correction of protected health information (PHI), University of Florida (UF) personnel must make reasonable efforts to verify the identity of any person making such requests. If the person making the request is not the patient, reasonable efforts should be made to also verify the authority of that person to have access to or to use the information. (See also SECTION 3: Uses and Disclosures of PHI: Family Members and Friends in this manual.)

2. Evidences of Identity: UF personnel should accept, and may reasonably rely on, any relevant evidence that appears reliable and reasonable under the circumstances, including, but not limited to, documents and other written representations, verbal statements or other oral representations, from the person making the requests described above, to substantiate a claim of identity and/or authority, unless the staff member has knowledge that there is a problem with the evidence being supplied.

3. Personal Representatives: UF will treat a patient’s personal representative(s) as the patient, as appropriate and within reason, as it relates to PHI that is relevant to such personal representation and only as allowed under the Privacy Rule and other applicable laws. UF reserves the right to refuse to recognize a personal representative’s authority if, in using professional judgment, such action is deemed in the patient’s best interests.

4. Delivery Options for Requests: Persons making requests concerning PHI are not required to present their requests in person, but may deliver them via mail or fax; signed documents may also be scanned and e-mailed to the appropriate record custodian.

NOTE: Verification is not required for appropriate actions if there is reasonable belief of an imminent threat to the safety of the patient or another individual.

B. DEFINITIONS

1. Family member: with respect to an individual, a family member means:
   a. A dependent (as such term is defined in 45 CFR 144.103) of the individual; or
   b. Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

   1) First-degree relatives include parents, spouses, siblings, and children.
   2) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES
1.5. Verification of Identity and Authority and Personal Representatives (continued)

3) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
4) Fourth-degree relatives include great-great-grandparents, great-great-grandchildren, and children of first cousins.

2. **Incapacitated Adult:** A person over the age of 18 who has been deemed incompetent by a court, or determined by an attending physician to be incapable of making informed health care decisions: Either situation must be documented in the patient’s health record.

3. **Personal Representative:** A person acting on behalf of the patient who must be treated as the patient for the purposes of the privacy regulations.

4. **Public Official:** A person elected or appointed to carry out some portion of a government's sovereign powers, including, but not limited to representatives of state health oversight and benefits agencies.

5. **Verification of Identity:** The process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information.

**C. PRIVACY REQUIREMENTS**

1. **Verification Requirements:** Prior to any disclosure of PHI permitted by the Privacy Rule (except for those uses and disclosures which require an opportunity for the individual to agree or to object), a covered entity must:

   a. Verify the identity of a person requesting PHI and the authority of any such person to have access to it, if the identity or any such authority of such person is not known to the covered entity; and

   b. Obtain documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such is a condition of the disclosure. If a disclosure is conditioned by the Privacy Rule on particular documentation, statements, or representations from the person requesting the PHI, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

2. **Exercise of Professional Judgment:** The verification requirements are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure, or acts on a good faith belief in making a disclosure in accordance with the applicable rules.

3. **Identity and Authority of Public Officials:** A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity and authority of a public official:

   a. **Identity:** Presentation of an agency identification badge, other official credentials, or other proof of government status, in person; or a written request on the appropriate government letterhead, or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.5. Verification of Identity and Authority and Personal Representatives (continued)

b. Authority: A written statement of the legal authority under which the information is requested or a properly executed warrant, subpoena, or judicial or administrative order.

4. Adults and Emancipated Minors: If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative, with respect to PHI relevant to such personal representation.

5. Unemancipated Minors: If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, with certain exceptions and restrictions.

6. Abuse, Neglect, Endangerment Situations: Notwithstanding a State law or any requirement of the Privacy Rule to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

a. The covered entity has a reasonable belief that:
   1) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
   2) Treating such person as the personal representative could endanger the individual; and

b. The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual’s personal representative.

7. Deceased Individuals: If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation. (See also SECTION 3: Uses and Disclosures of PHI: Family Members and Friends in this manual.)

D. PROCEDURES

1. Provide Assistance as Needed: Assist the person making a request regarding PHI to complete the appropriate form for the request (see Forms).

   a. Release of information: complete an Authorization to Use or Disclose Health Information,

   b. Restrictions of PHI or more confidential communications: complete a Request for Special Privacy Restrictions,

   c. Correcting/adding information in a record: complete a Request for Amendment of a Health Record,

   d. Accounting of disclosures of PHI: complete a Request for an Accounting of Disclosures

2. Document on the completed form how the identity and authority of anyone requesting PHI was verified. If there are any doubts, refer to your immediate supervisor.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.5. Verification of Identity and Authority and Personal Representatives (continued)

   a. If the person is known, document the basis of knowledge of both identity and authority as “known patient”, “long-time patient”, “parent of established patient”, etc., as appropriate.
   b. For a personal representative, document proof of status as parent (if available), guardian, health care surrogate, health care power of attorney, executor, administrator, etc.
   c. For public officials, document either the presentation of proof of government status, such as official credentials, a badge or identification card, or the official’s oral representation: what was said and why it was considered reasonable to rely on it.
   d. For law enforcement or legal processes: receive the written warrant, subpoena, order, summons, or civil investigation demand presented, and refer the request to your immediate supervisor.
   e. For research: refer to your immediate supervisor. (Proper documentation from an Institutional Review Board, other appropriate privacy board, or the researcher relating to research must be presented).
   f. For all others, request a common form of identification, preferably one that includes a photo of the requestor, and document the information on the authorization or request form.

3. Verifying the Identity of a Patient or of a Personal Representative:

   a. When a patient or personal representative appears in person, ask for identification if the person is not known. The following may be reasonably relied on as meeting the requirements of verification of identity, including, but not limited to:
      1) Personal knowledge of an individual, place of business, address, or phone or fax number.
      2) Documents presented by the patient or representative, including a picture-identification card, a state-issued driver’s license, a photo-ID credit card, or a government issued passport.
      3) Other reasonable written or oral evidence: document the reasons why the evidence is considered valid and reasonable for identification.
   b. When individuals call in by telephone, ask for the specific personal identification information about the patient, which has been defined by your clinic, department, or unit as meeting the requirements of verification of identity. A pre-arranged password or security code, in addition to the patient’s full name may also be used.
   c. When individuals send in requests by mail or other methods, staff may reasonably rely on documentation provided by the requestor, unless staff members know there is a problem with the documentation. When in doubt, staff members can ask for more definitive proof of identity, or refer the request to the clinic, department, or unit manager or to the Privacy Office.

4. Verifying the Authority of a Personal or Legal Representative:

   a. Minors (Non-emancipated): For the purposes of HIPAA and access to PHI, natural or adoptive parents, legal custodians, and legal guardians are the personal representatives of persons under the age of 18.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.5. Verification of Identity and Authority and Personal Representatives (continued)

Exceptions: The following are some, but not all, cases in which parents or guardians of minors would not be considered personal representatives, and therefore not authorized to access the patient’s PHI without the minor patient's authorization:

1) When the minor requests a medical examination or testing for STDs (including HIV);
2) When a minor voluntarily self-admits into a substance abuse facility;
3) When the minor is emancipated;
4) When a minor requests outpatient mental health diagnostic/evaluation services (> age 13);
5) When a minor requests outpatient crisis intervention therapy/counseling services (> age 13).

b. Emancipated Minors: For purposes of HIPAA and access to PHI, the following persons under the age of 18 do not need parental consent for any health care; their parents or guardians would not be personal representatives, unless so designated by the minor:

1) Unmarried minor female consenting to health care relating to her current pregnancy;
2) Unmarried minor female consenting to health care for her minor child;
3) Married minor (including widowed and divorced);
4) Minor emancipated by court order;
5) Minor enlisted in military service.

c. Incapacitated Adults: For purposes of HIPAA and access to PHI, legal representatives are usually appointed and able to produce documents; they include:

1) Court-appointed Guardian;
2) Durable Power of Attorney (DPOA): Appointed by the patient, with authority defined. Read the DPOA to determine authority to access PHI; if not stated specifically, access is not included.
3) Healthcare Surrogate: Appointed by the patient, but usually not effective until the patient is declared mentally or physically incapacitated by a specified number of physicians. Read the document to determine the effective date or event and other relevant criteria.
   a) Authority to make health care decisions automatically includes access to PHI.
   b) Authority to act may be limited, that is, the authority may be specified as only for purposes of end-of-life decisions or other defined circumstances. Read the document to ascertain the scope of authority.
4) Health Care Proxy: When an incapacitated patient has not personally appointed a substitute decision-maker (DPOA for Health Care or Health Care Surrogate), the following persons, in order of priority, may be appointed by UF, in accordance with Florida law, as Health Care Proxy. The appointment must be documented in the patient’s health record, including efforts to locate proxies from prior classes.
   a) Judicially appointed guardian;
   b) Patient’s (current and legal) Spouse;
   c) Adult child of the patient, or a majority of adult children reasonably available;
   d) Parent of the patient;
   e) Adult sibling of the patient, or a majority of adult siblings reasonably available;
   f) Adult relative of the patient who has exhibited concern and maintained contact;
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.5. Verification of Identity and Authority and Personal Representatives (continued)

g) Close friend of the patient.

5. **Representatives for deceased patients:** Refer requests for decedents’ health information to your supervisor or the Privacy Office. The following are guidelines for identifying legal representatives:

a. **With a Will:** The Executor of the Estate is the personal representative.

b. **Without a Will:** If no personal representative was named, the following persons, in order of priority, can serve as personal representatives:

1. The surviving spouse
2. A person selected by a majority of those persons entitled to a share in the estate under the laws of intestate succession (i.e. lineal descendants, father and mother, siblings)
3. An heir in the nearest degree to the decedent (if more than one, the court appoints a representative)

E. **REFERENCES:**

1. **HIPAA:** 45 CFR § 160.103 Definitions; §164.502(g) Personal Representatives; §164.514(h) Other Requirements: Verification

2. **Florida Statutes:** 384.29 Sexually Transmissible Diseases: Confidentiality; 394.459 Mental Health: Rights of Patients; 395.501 Substance Abuse: Rights of Individuals; 395.601 Substance Abuse: Voluntary Admissions; 709.08 Durable Power of Attorney; 765 Health Care Advance Directives

F. **EXHIBITS**

None
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.6. Minimum Necessary Rule

**A. POLICY**

1. **Setting Limitations:** University of Florida (UF) healthcare providers and staff must make every effort to reasonably limit uses, disclosures, and requests for protected health information (PHI) to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
   
   a. *All staff members* are responsible for knowing and following their departments’ minimum necessary procedures.
   
   b. *The entire health record* should not be used, disclosed or requested unless it is specifically required for the intended purpose and/or for treatment of the patient.

2. **Limiting Uses:** UF departments, clinics, and other units should identify, by role, persons or entities that need access to PHI to carry out their assigned job duties;
   
   a. *Categories of PHI to which access is needed* must be identified and any conditions appropriate to such access clearly defined.
   
   b. *All access to PHI* must be documented and all staff must be educated about their department’s minimum necessary procedures.

3. **Limiting Disclosures and Requests:** Departments should develop and maintain a list of categories of persons and organizations to which PHI is routinely disclosed and/or from which information is routinely requested, the purpose of the disclosures and requests, and the minimum information needed for each purpose.
   
   a. *Routine Disclosures and Requests:* Disclosures and requests classified as “Routine” should only be for treatment, payment, and health care operations. Personnel may rely on a health care provider’s request for information for treatment to be the minimum necessary for the purpose.
   
   b. *Non-Routine Disclosures* should be authorized only after review of the request, verification of the requestor’s identity and authority to receive PHI, and a review of the minimum necessary criteria. Designated personnel in each department should be able to use the “Minimum Necessary Decision Tree” to identify persons or entities, who do not routinely request information, as either meeting or not meeting the specifications for the minimum necessary rule.
   
   c. *Non-Routine Requests:* should be analyzed carefully to determine the minimum necessary information needed to fulfill the purpose. Any PHI requested from another person or organization that is not specifically for treatment should only be made with the patient’s authorization.

**B. DEFINITIONS**

- **Minimum Necessary:** HIPAA does not define this term.

- **Professional Need to Know:** Specific, limited, and usually specialized information necessary to complete assigned work.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.6. Minimum Necessary Rule (continued)

C. PRIVACY REQUIREMENTS

1. Minimum Necessary applies: When using or disclosing PHI or when requesting PHI from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

2. Exemptions to the Minimum Necessary Rule: “Minimum Necessary” does not apply to the following uses, disclosures, or requests:
   a. By or to a health care provider for treatment
   b. By or to the individual who is the subject of the information
   c. In response to a valid authorization by the patient/representative
   d. For HIPAA-mandated transactions
   e. By or to the Department of Health and Human Services (HHS)
   f. When and as required by law

3. Minimum Necessary uses of PHI:
   a. A covered entity must identify:
      1) Those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties; and
      2) For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.
   b. A covered entity must make reasonable efforts to limit the access of such persons to PHI.

4. Minimum Necessary disclosures of and requests for PHI: For any type of disclosure or request made on a routine and recurring basis, a covered entity must implement policies and procedures that limit the PHI disclosed or requested from other covered entities to the amount reasonably necessary to achieve the intended purpose. For all other (non-routine) disclosures and requests, a covered entity must develop criteria to limit the PHI, disclosed and requested, to what is reasonably necessary, and review disclosures and requests on an individual basis in accordance with such criteria.

5. A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:
   a. Making disclosures to public officials as permitted in #2 above, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);
   b. The information is requested by another covered entity;
   c. The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.6 Minimum Necessary Rule (continued)

d. Documentation or representations that comply with applicable requirements have been provided by a person requesting the information for research purposes.

6. For all uses, disclosures, or requests, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount reasonably necessary to accomplish the purpose of the use, disclosure, or request.

D. PROCEDURES

1. Limiting Uses: Refer to the departmental list that identifies persons by role, and the types of PHI to which each role has access. Do not use the entire health record unless it is specifically authorized or required for the intended purpose.

2. Limiting Disclosures: Do not disclose the entire health record unless it is specifically warranted as the amount reasonably needed for the purpose of the disclosure, or it has been authorized by the patient.

   a. Routine Disclosures: Refer to your department’s list of persons and organizations to which your department routinely discloses PHI. Limit the amount of information disclosed to the minimum needed in each case to fulfill the purpose.

   b. Non-Routine Disclosures: Use the “Minimum Necessary Decision Tree” to identify persons or entities, who do not routinely request information, as either meeting or not meeting the specifications for the minimum necessary rule.

      1) Verify the identity and authority of the requestor, and obtain authorization from the patient or a supervisor before releasing any information, if the disclosure is not routine.

      2) The minimum necessary rule does not apply to a health care provider’s request for information for treatment purposes. Disclose, within the limitations of other state and federal laws, any amount of information that is requested for treatment.

3. Limiting Requests: Do not request an entire health record unless it is specifically required for treatment of the patient.

   a. Routine Requests: should only be for treatment, payment, and health care operations. Workforce members are responsible for helping maintain:

      1) A list of categories of persons or places from whom PHI is routinely requested,

      2) The routine purpose of the requests,

      3) The minimum information necessary to meet each request.

   b. Non-Routine Requests: Obtain the patient’s authorization before requesting PHI from another provider or covered entity, if it is not specifically related to treatment.

E. REFERENCES:

HIPAA: 45 CFR §164.502(b) General Rules: Minimum Necessary; §164.514(d) Other Requirements: Minimum Necessary
**SECTION 1: GENERAL HIPAA AND PRIVACY RULES**

1.6. Minimum Necessary Rule (continued)

**F. EXHIBITS**

1. Minimum-Necessary Decision Tree
2. Examples of Routine and Non-Routine Disclosures and Requests

**Minimum-Necessary Decision Tree:**

<table>
<thead>
<tr>
<th>ASK:</th>
<th>If the answer is “NO”</th>
<th>If the answer is “YES”</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Is the intended use, request, or disclosure being made for or by, a healthcare provider for treatment purposes?</td>
<td>Go to the next question</td>
<td>The Minimum Necessary Rule does NOT apply.</td>
</tr>
<tr>
<td>2) Is the use or disclosure being made to the individual who is the subject of the PHI?</td>
<td>Go to the next question</td>
<td></td>
</tr>
<tr>
<td>3) Is the use and disclosure being made in response to a valid authorization?</td>
<td>Go to the next question</td>
<td></td>
</tr>
<tr>
<td>4) Has HHS requested disclosure for HIPAA compliance and enforcement?</td>
<td>Go to the next question</td>
<td></td>
</tr>
<tr>
<td>5) Is the use or disclosure required by law (reporting abuse, neglect or domestic violence, responding to a subpoena or court order, or in response to a law enforcement officer investigating a crime)?</td>
<td>Then the information to be used, disclosed, or requested must abide by the minimum necessary rule. Verify identity and authority, if appropriate.</td>
<td>Then certain other restrictions apply under HIPAA, but not the Minimum Necessary Rule.</td>
</tr>
</tbody>
</table>
## SECTION 1: GENERAL HIPAA AND PRIVACY RULES

### 1.6. Minimum Necessary Rule (continued)

#### Examples of Routine and Non-Routine Disclosures and Requests

<table>
<thead>
<tr>
<th>Routine Disclosures</th>
<th>What to Disclose</th>
<th>Routine Requests</th>
<th>What to Request</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Treatment Purposes</strong></td>
<td>Disclosures associated with routine referrals to local Laboratories, Pharmacies, Rehab Facilities, etc.</td>
<td>Generally limit PHI to patient name, demographics, appropriate diagnosis information, and reason for referral/prescription</td>
<td>Requests for PHI from Referring Physicians and other Health Care Practitioners</td>
</tr>
<tr>
<td><strong>Payment Purposes</strong></td>
<td>Disclosures for Billing/Reimbursement Purposes</td>
<td>Limit information to records for the date of service in question.</td>
<td>Requests for Pre-approval and Eligibility Determinations</td>
</tr>
<tr>
<td><strong>Required By Law</strong></td>
<td>Disclosures for Public Health Activities</td>
<td>Limit information to the specific data required by the database or agency. Only related to the specific incident being reported or investigated. Additional info, including the pat’s health history may only be disclosed by court order, subpoena, or under other applicable statutes or laws.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-Routine Disclosures</th>
<th>What May Be Disclosed</th>
<th>Non-Routine Requests</th>
<th>What May Be Requested</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Treatment Purposes</strong></td>
<td>Emergency Disclosures of Health Information Needed for Treatment</td>
<td>Any information available under current relevant laws. Minimum Necessary does not apply.</td>
<td>Emergency Requests for Health Information Needed for Treatment</td>
</tr>
<tr>
<td><strong>Payment Purposes</strong></td>
<td>Disclosures for Billing/Reimbursement Activities of another health care provider</td>
<td>Disclose no information without patient’s authorization.</td>
<td>Requests for Billing/Reimbursement Activities of another health care provider</td>
</tr>
<tr>
<td><strong>Required By Law</strong></td>
<td>Disclosures in Response to Court Orders and Subpoenas:</td>
<td>Limit disclosures to the specific information indicated in the order.</td>
<td></td>
</tr>
</tbody>
</table>
SECTION 1: GENERAL HIPAA AND PRIVACY RULES
1.7. Education and Training

A. POLICY

1. Training and Education regarding Privacy and Security of Health Information is required for all members of the University of Florida (UF) workforce in health care components. Training is provided by UF as follows:

   a. **HIPAA Privacy and Security: General Awareness Training**
      1) For each new member of the workforce, to be completed within the first 5 - 10 business days after the person joins the workforce;
      2) For official visitors to UF’s health care components and any other patient care areas, to be completed prior to beginning activities at UF.
      3) Required Annual Renewal by all members of the workforce.

   b. **Supplemental Role-based HIPAA and Privacy Training** for workforce members based on their position and/or responsibilities, including:
      1) Policies and Procedures Training for faculty, staff, students, and volunteers.
      2) HIPAA for Researchers for all members of human subject research teams.

   c. **Focused HIPAA Privacy and Security Training** for members of the workforce whose functions are specialized, requiring more narrow or in-depth training.

   d. **Update HIPAA Privacy and Security Training** for members of the workforce whose functions are affected by a material policy or procedure change, within a reasonable period of time after the change becomes effective.

2. Documentation: UF maintains electronic records of training provided to all workforce members for the retention period prescribed in the HIPAA Privacy regulations.

3. Scope of Participation: All members of the UF workforce in health care components are required to complete an appropriate training module, review the Health Information Policy and sign the Confidentiality Statement at orientation and annually.

   a. **Failure to comply** with the training requirements is a Level Two (2) Privacy violation.

   b. **Failure to complete the requirements** within 60 days after joining the workforce or the annual renewal due dates will result in:
      1) Loss of access to hospital and other computer systems for those who have such access. Access will not be reinstated until the required training has been completed and the training certificate hand-delivered to the Privacy Office.
      2) For those who do not have computer access, a mandatory meeting with the Chief Privacy Officer and the employee’s immediate supervisor.
      3) Disenrollment or suspension from classes for students.
      4) Other sanctions as prescribed by policy may also be imposed.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.7. Education and Training (continued)

4. **Personal and Departmental Responsibilities:** Each individual, as a member of the workforce, is ultimately responsible for maintaining personal compliance with UF’s Privacy training requirements. Supervisors in all colleges, departments, divisions, and clinics are responsible for maintaining records of training compliance for all workforce members. Other responsibilities include:
   a. *Incorporating appropriate training* into interviewing, hiring and orientation procedures for new staff, students, and volunteers,
   b. *Making all workforce members aware* of any changes in Information Privacy and Security training requirements, and
   c. *Ascertaining* that workforce members have completed all training requirements.

**B. DEFINITIONS**

1. **Workforce:** University of Florida (UF) faculty, staff, students, volunteers, trainees, and any other person, including, but not limited to, visiting and associate clinicians, visiting faculty, Business Associates, and other persons performing services for UF, whether temporary or permanent, whose conduct, in the performance of work with or for UF, is under the University’s direct control, regardless of whether the person is paid for their services or not.

2. **Visitors:** Any person who is not formally associated with UF health care components including, but not limited to:
   a. Trade representatives,
   b. Maintenance technicians,
   c. Visiting health care professionals,
   d. Visiting students (including non-HSC UF students),
   e. Visiting family members of UF employees,
   f. Applicants for UF positions,
   g. Any other similar persons or groups.

   *NOTE:* “Visitors” do not include UF students who are enrolled in a Health Science Center College or Program, volunteers working for the HSC, patients, or family members or friends visiting or accompanying patients.

**C. PRIVACY REQUIREMENTS**

1. **Security awareness and training.** A covered entity or business associate must implement a security awareness and training program for all members of the workforce (including management).

1. **Privacy Standard: training.** A covered entity must train all members of its workforce on the policies and procedures with respect to PHI required by the Privacy Rule, as necessary and appropriate for the members of the workforce to carry out their functions.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.7. Education and Training (continued)

   a. A covered entity must provide training to each new member of the workforce within a reasonable period of time after the person joins the covered entity’s workforce; and to each member of the covered entity’s workforce whose functions are affected by a material change in the policies or procedures within a reasonable period of time after the material change becomes effective.

   b. A covered entity must document that the training has been provided.

D. TRAINING PROGRAMS

1. Level One Training: General Awareness

   a. **HIPAA & Privacy: General Awareness** (may be replaced by Research and Information Privacy; see b. below.)

      1) Participants include, but are not limited to the following, whether they have contact with patients or PHI or not.

         a) All members of the workforce as defined in this policy;
         b) Visiting and associate faculty, students, and other persons performing services for UF;
         c) Business associates, as needed.

      2) Frequency:

         a) At orientation or other entry into the UF workforce.
         b) Annually, during January and February for faculty and staff, and during May, June, July and August for students.

      3) Content: Introduction to Information Privacy and Security

         a) Privacy, Confidentiality and Security
         b) Scope of Privacy Regulations: Workforce, Covered Entities and PHI
         c) Privacy Obligations and Requirements
         d) Reporting and Responding to Privacy Complaints and Violations
         e) Patient’s Rights under HIPAA
         f) HIPAA and Florida Statutory Privacy Requirements
         g) Sanctions for Violations of Privacy

   b. **Research and Information Privacy – HIPAA for Researchers** (may be completed in place of HIPAA & Privacy: General Awareness; see a. above.)

      1) Participants: All personnel involved in human subject research activities; including, but not limited to:

         a) Principal investigators, co-principals and sub-investigators,
         b) All research coordinators,
         c) All staff with access to research-related PHI.

      2) Frequency: Prior to submitting new research protocols, and annually thereafter during the regular annual privacy renewal training (January and February), as long as the participants are involved in human subject research. Failure to maintain current training certification may be cause for rejection, suspension, or significant delay of a research protocol under review.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.7. Education and Training (continued)

3) Content: Privacy and Security General Awareness Training plus:
   a) Individually Identifiable Information
   b) De-identification
   c) Authorizations / Waivers / Certificates
   d) Retention of documentation

2. Level Two Training: Health Information Privacy Policies and Procedures
   a. Participants: Administrative and Management Clinical and Non-Clinical Personnel who may have
      contact with PHI, or who supervise persons who have contact with patients and/or PHI.
   b. Frequency: At orientation, and as needed thereafter, relative to changes in policies and/or changes
      in roles or job descriptions.
   c. Content:
      1) Reporting and Responding to Privacy Complaints and Violations
      2) Health Information and Record Management Policies
      3) Patient’s Rights Procedures & Verification of Identity and Authority
      4) Uses and Disclosures of PHI & Minimum Necessary Rule
      5) Accounting for Disclosures

3. Level Three Training: Role-Specific Tutorials
   a. Notice of Privacy Practices – Optional training
      1) Participants: All personnel who have first contact with patients
      2) Frequency: At orientation, and as needed thereafter, relative to changes in policies and/or
         changes in roles or job descriptions.
      3) Content
         a) Purpose and Content of the Notice; answering Patients’ questions
         b) Procedures for providing the notice and obtaining acknowledgement
   b. Disclosure Tracking & Accounting – Mandatory training for designated staff
      1) Participants: Only designated personnel authorized to enter data in UF’s On-Line Disclosure
         Tracking System.
      2) Frequency: Prior to receiving access to the system, annually, and as needed thereafter, relative
         to changes in policies and/or changes in roles or job descriptions.
      3) Content: Privacy and Security General Awareness plus:
         a) Purpose of the Disclosure Tracking System
         b) Disclosures that must be entered in the system
         c) General instructions for use of the system
   c. HIPAA for Fundraisers - Mandatory training for designated staff
      1) Participants: Personnel in HSC development offices involved in fund-raising and donor relations
         with patients.
SECTION 1: GENERAL HIPAA AND PRIVACY RULES

1.7. Education and Training (continued)

2) Frequency: During new-hire orientation, annually, and as needed thereafter, relative to changes in policies and/or changes in roles or job descriptions.

3) Content:
   a) UF’s privacy protection policies for patients
   b) Federal Trade Commission rules and regulations
   c) Other federal and state laws
   d) Procedures for fundraising

E. PROCEDURES

1. Online Self-Directed Training Modules
   a. Access and enroll in the appropriate on-line Training Program through the myUFL web site: https://my.ufl.edu/ps/signon.html, My Self-Service, Training and Development; myTraining Enrollment
   b. Successfully complete the training module and obtain a passing score on the quiz.
   c. Print the Certificate of Completion, if provided (not all training modules provide a certificate).

2. Face-to-Face Health Information Privacy Policies and Procedures Training: Include in orientation to any new position; repeat as and when needed. Supervisors should:
   a. Present or coordinate the employee’s attendance at, or completion of, necessary Level Two Privacy and Security training, either as on-the-job, self-directed, or classroom instruction, as appropriate.
   b. Document the amount of training presented and include the record in the individual’s personnel file.

F. REFERENCES:

HIPAA: 45 CFR §164.308 (a)(5)(i) - Security Training, §164.530(b)(1) and (2) - Privacy Training

G. EXHIBITS:

None
### SECTION 2: HEALTH INFORMATION MANAGEMENT

#### 2.1. General Policies

<table>
<thead>
<tr>
<th><strong>A. POLICY</strong></th>
<th>REV. 07/01/2012</th>
</tr>
</thead>
</table>

1. **Maintenance and Ownership of Healthcare Records and UF’s Commitment:**
   a. Health and financial records created as a result of patient care encounters in any University of Florida (UF) patient care area, including faculty practice clinics in Gainesville, Jacksonville, and outlying areas, the Student Health Care Center, and the Counseling and Wellness Center, are the property of UF, even though components of the records may be shared with the Shands HealthCare System.
   b. A health record shall be maintained for every individual who is evaluated or treated as a patient in any UF patient care area. Currently, UF’s health records are considered hybrid records, consisting of both electronic and paper documentation.
   c. Information recorded in UF’s healthcare and patient financial records ultimately belongs to the patients about whom it is recorded. UF is committed to protecting the confidentiality of all patient information it receives, creates, maintains, and transmits in any format.

2. **Confidentiality and Availability of Records:** Health information is confidential and is protected from unauthorized disclosure by law. It is available for use by:
   a. UF faculty, residents/fellows, staff, and authorized volunteers working within the UF and Shands Organized Health Care Arrangement, when acting within the course and scope of their official duties related to UF business. (See **SECTION 2: HIM: Documentation Rules** for more details.)
   b. Authorized students enrolled in healthcare and health-related education programs of, or affiliated with, UF. (See **SECTION 6: Student Data Access** policy in this manual.)

3. **Content of Health Records:** Health record content shall meet all State and federal legal, regulatory and accreditation requirements including but not limited to those related to physician, dental and other professional healthcare provider practices.

4. **Use and Disclosure of Protected Health Information (PHI):** Individually identifiable health information created, received, maintained, or transmitted by UF in any format may only be used and disclosed in accordance with federal and state laws and UF’s policies and procedures or with the approval of the Chief Privacy Officer. (See **SECTION 3: Uses and Disclosures of PHI: General Rules** in this manual.)

5. **Removal of Patient Related Information:** Patient information, whether original or copied, in paper or electronic formats, that is generated or received for the care of patients by UF, may NOT be removed from the premises of UF or Shands by anyone, except upon receipt of a court order, subpoena duces tecum, or written departmental administrative approval.

6. **Health Information Custodians:**
   a. The Chief Privacy Officer is the officially designated Custodian for Health Information Records in all formats for UF in all locations. The Chief Privacy Officer may delegate these custodial duties as appropriate.
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.1. General Policies (continued)

b. Any issues with UF records related to patients’ rights (i.e., requests for copies, amendments, restrictions, etc.) or other requests for copies or information are managed by designated UF health information management personnel.

c. Shands Healthcare is the delegated record custodian for a very limited group of UF medical clinics; questions about custodianship should be directed to the UF Privacy Office. (See SECTION 2: Health Information Management: Record Custodian List in this manual.)

7. Health Information Management Personnel: Each patient care area and department that creates, receives, maintains, uses, and/or discloses PHI in any format must designate at least one staff member to manage the health information and patient records for that area. The staff member is not required to be solely dedicated to the management of health information, but must be specifically trained and responsible for maintaining the confidentiality, security, and accessibility of patients’ information.

B. DEFINITIONS

1. Active/Inactive Records: Active healthcare records are those currently being used for ongoing patient care, payment, litigation, or research activities. Inactive records are those for patients who have not received healthcare, made payments for care, or been involved in litigation or research for a designated period of time.

2. Designated Record Set: A defined group of health and billing records that contain PHI. (See Appendix A: Glossary for full definition; see also Exhibits: Designated Record Set chart in this chapter.)

3. Legal Health Record (LHR): A formally defined legal business record, made by a healthcare organization, in the routine course of business at or near the time that events occurred. The legal health record is a subset of the entire patient database, and identifies what information constitutes the official business record of an organization for evidentiary purposes.

   a. The legal health record is comprised of individually identifiable data, recorded in any medium, collected from multiple disciplines, and used by healthcare professionals while providing patient care or services, reviewing patient data, or documenting observations, actions, or instructions.

   b. Documentation may include personal identification information, diagnoses, treatments, services provided, and payment for services. Documentation may also include copies of records, created elsewhere, that are considered relevant to decisions made about care or services provided at UF.

   c. Components of the legal health record may physically exist in separate and multiple paper-based files or electronic/computer-based databases; these components would be compiled and released upon receipt of a legally authorized request.

4. Primary Records: Original documentation created and maintained in any format as a direct result of a patient or client encounter in any of UF’s healthcare facilities, including faculty practice clinics and student health clinics. Paper Primary records are usually maintained in and/or by the entity where the care or service was provided. Primary records also include any original documents that are not reproducible elsewhere, such as older records being retained in off-site storage.
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.1. General Policies (continued)

5. **Shadow Records:** Paper copies of primary records that are temporarily kept separately from the primary record, usually for the convenience of health care providers or their staff. Shadow records should not be created in areas where electronic records are available.

   **NOTE:** Paper records that were created and maintained in UF clinics are not shadow records, even though they may include documents shared with other parts of UF and Shands.

---

C. PRIVACY REQUIREMENTS

1. **Using and Disclosing Health Information:** Individually identifiable health information created, received, maintained, or transmitted by UF may only be used and disclosed in accordance with UF’s policies and procedures or with the approval of the Chief Privacy Officer.

2. **Authorizations:** A complete and valid Authorization (see Forms) is required for disclosures of PHI for purposes not related to treatment, health care operations, or as otherwise required by law, including:
   a. To patients or their legal representatives (See SECTION 4: Patient’s Rights - Access to Personal Health Records in this manual.)
   b. To third parties, including healthcare professionals who do not have a treating relationship with the patient (See SECTION 3: Uses and Disclosures of PHI - Authorizations in this manual.)
   c. To researchers (See SECTION 3: Uses and Disclosures of PHI - Research in this manual.)

3. **Security of Active Records:** All patient records in all formats must be stored so that they are available for use, but also physically and technologically secure. Information and records must be protected from unauthorized access, physical damage by fire, water, insects, pests, temperature, and humidity, and other reasonably foreseeable hazards. (See also UFP Epic Policies on the UFP website, and Shands HIM Policies on the UF Health Shands website).

---

D. PROCEDURES

1. **Health Record Integrity and Chronology:** Double check to be sure paper documents are filed in the correct patient’s record in chronological order and that electronic information and scanned/imaged documents are being entered in the correct encounter record for the correct patient.

2. **Authorized Disclosure/Release of Health Information:** Route all requests related to disclosure of PHI to the designated record manager for the primary record. Only authorized personnel who have been appropriately trained should disclose patient information in response to requests. (See SECTION 3: Uses and Disclosures of PHI: General Rules in this manual,)

3. **Specific Procedures:** Refer to your college, department or unit policies and procedures developed for specific Health Information Management issues, especially as related to electronic health records.

4. **Disaster Preparations:** Refer to your facility’s Disaster Manual for protection of non-electronic records during potentially damaging situations. Refer to UF’s Information Security Guidelines and your unit’s Information Security Manager for protection of electronic records.
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.1. General Policies (continued)

E. REFERENCES:

1. HIPAA: 45 CFR §164.501 - Definitions; § 164.502 - Use and Disclosure
2. Florida Statues: 456.057 - Ownership and Control of Patient Records

F. EXHIBITS

1. The Designated Record Set
2. Records Custodians for UF and Shands Clinics

Back to Table of Contents
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.1. General Policies (continued)

The Designated Record Set

<table>
<thead>
<tr>
<th>Included in the Designated Record Set</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Health records created, received, maintained, or transmitted by healthcare providers in UF’s health care components. | • The content of any paper-based and/or electronic patient health record held by UF;  
• UF Student Health Records, except immunization records. |
| Billing records created, maintained, or transmitted by health care providers in UF’s health care components. | • The content of any paper-based healthcare account record held by UF;  
• Any patient account data in a computerized scheduling system, or electronic billing and accounting system. |
| Other records used to make health care decisions about the individual. | • A clinical report generated by a hospital physician and subsequently incorporated into a UF patient health record;  
• Copies of reports generated by other UF providers and used to make decisions about the individual, even when kept in shadow charts. |
| Records maintained by a business associate that meet the definition of designated record set that are not duplicates of records maintained by the covered entity. | • Records maintained by record storage companies that have agreed to manage release of information rather than returning the records to the covered entity to respond. |
| Source data interpreted or summarized in the individual’s medical or health record. | • Interpretations of Pathology slides;  
• Interpretations of Diagnostic films;  
• Interpretations derived from Electrocardiogram tracings. |

<table>
<thead>
<tr>
<th>Not in the Designated Record Set</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Health information generated, collected, or maintained for purposes that do not include decision-making about the individual. (Copies of patient records from other providers that were not used to make health care decisions about the patient, if retained, are available for inspection only, not copying) | • Data collected and maintained for research, peer review (QA/QI); or performance/outcomes improvement purposes;  
• Appointment and surgery schedules;  
• Diagnostic or operative indexes;  
• Duplicate copies of information that may also be located in the individual’s official health or billing record. |
| Psychotherapy notes. | • The notes of a mental health professional about counseling sessions that are maintained separate and apart from the regular health record. |
| Information compiled in anticipation of, or for use in a civil, criminal, or administrative action or proceeding. | • Notes taken during a meeting with our attorneys about a pending lawsuit. |
| CLIA Documents | • Requisitions for laboratory tests;  
• Duplicate lab results when the originals are filed in the individual’s primary health record. |
| Employer records when patient is a UF / UFP / UFJHI / UFJPI / SHCC employee. | • Pre-employment physicals and employee health records (immunization, PPD, etc.) maintained in Human Resources files.  
• The results of HIV tests maintained by the infectious disease control nurse on employees who have suffered needle stick injuries on the job. |
| Business associate records that duplicate information maintained by the covered entity. | • Transcribed operative reports transmitted to the covered entity. |
| FERPA Student Health Records | • Immunization Records |
| UAA Student Athlete Records | • Pre-Participation Physicals, drug-testing and immunization records, insurance info, diagnostic test results, progress notes, rehab notes, physician dictations, health referral and notes |
| Source Data (Available for copying or inspection upon the specific request of the patient) | • Pathology slides  
• Diagnostic films  
• Electrocardiogram tracings from which interpretations are derived |
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.1. General Policies (continued)

Medical Record Custodians for UF Physicians (UFP) and Shands Clinics

UF HEALTH SHANDS is the record custodian for the following areas: Record requests may be sent to Shands HIM

<table>
<thead>
<tr>
<th>Shands Units</th>
<th>UF Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blood Bank</td>
<td>Cardiovascular Med Clinic – Shands 1st floor only</td>
</tr>
<tr>
<td>Bone Marrow Center</td>
<td>Communicative Disorders – 2nd floor (PHHP)</td>
</tr>
<tr>
<td>Burn Clinic</td>
<td>ENT Clinic – Shands 1st floor only</td>
</tr>
<tr>
<td>Dietary Services</td>
<td>Endocrinology Clinic – Med Plaza</td>
</tr>
<tr>
<td>Emergency Department</td>
<td>Gastroenterology Clinic / Endoscopy Center</td>
</tr>
<tr>
<td>Endoscopy Centers</td>
<td>Infectious Disease Clinic – Med Plaza</td>
</tr>
<tr>
<td>Florida Surgical Center</td>
<td>Nephrology Clinic – Med Plaza</td>
</tr>
<tr>
<td>Heart Station (EKG/Echo/Treadmill)</td>
<td>Neurosurgery Clinic – Shands 1st floor only</td>
</tr>
<tr>
<td>Infusion Center</td>
<td>Psychology (Inpatient only)</td>
</tr>
<tr>
<td>Pathology</td>
<td>Pulmonary Clinic – Med Plaza</td>
</tr>
<tr>
<td>OB (Deliveries only)</td>
<td>Radiation Oncology</td>
</tr>
<tr>
<td>PT/OT/Massage Therapy</td>
<td>Rheumatology Clinic – Med Plaza</td>
</tr>
<tr>
<td>Radiology</td>
<td>Transplant Services – Med Plaza</td>
</tr>
</tbody>
</table>

UF is the record custodian for these areas: Request records from the individual clinics or departments

<table>
<thead>
<tr>
<th>UF Clinics &amp; Centers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancer Center Clinics - ALL</td>
<td>Ophthalmology</td>
</tr>
<tr>
<td>Cardio-West Clinic</td>
<td>Orthopedics &amp; Sports Medicine</td>
</tr>
<tr>
<td>Child Psychiatry Clinic (Ground Floor)</td>
<td>Pediatric Clinics - ALL</td>
</tr>
<tr>
<td>Dermatology Clinic</td>
<td>Psychiatry / Pain Clinics - ALL</td>
</tr>
<tr>
<td>ENT Clinic – Hampton Oaks</td>
<td>Psychology Clinics (College of PHHP)</td>
</tr>
<tr>
<td>Family Practice / Family Medicine Clinics - ALL</td>
<td>Surgical Associates</td>
</tr>
<tr>
<td>Internal Medicine Clinics – except Medical Specialties @ Med Plaza</td>
<td>Urology</td>
</tr>
<tr>
<td>Neurology Clinic</td>
<td>Women’s Health - OB/GYN Clinics</td>
</tr>
</tbody>
</table>
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.2. Documentation Rules

A. POLICY

1. Authorization to Document: Only credentialed physicians and caregivers, UF and Shands employees acting within the scope of their assigned duties, authorized students, and contracted individuals with an equivalent competency process, are authorized to document in UF’s health records.
   a. Specific charting privileges of non-physician authors will be delineated and supervised by the department head or faculty member to whom the author reports.
   b. Documentation by Students: Authorized students must document under the direct supervision of a licensed or registered professional. The term “student” includes individuals participating in internship or practicum phases of degree programs affiliated with the UF Health Science Centers and affiliated colleges.

2. General Documentation Requirements:
   a. Paper Records
      1) Patient identification information (including name and record number) must be recorded on every page of each document.
      2) All handwritten entries must be written legibly in black or blue ink.
      3) The date and time must precede each entry,
      4) The signature of the author must follow all entries, including the author’s unique identification number and/or title. Stamped signatures are not allowed in health records.
   b. Electronic Records
      1) Providers are required to use the current electronic health record (EHR) system to provide readily accessible, timely, and accurate information for ongoing patient care. Providers should not create paper documents for permanent inclusion in a patient’s electronic health record. Providers may not print electronic documents to use during treatment, except in rare emergency situations.
      2) Logging in to the EHR system constitutes authentication for all entries.
      3) Patient identification information (including name and record number) must be verified before making any entry in a patient’s EHR.
      4) All hand-written notes must be retained and/or scanned into the EHR unless the information is dictated or duplicated in some other area of the health care record.
      5) Copy and Paste functionality, if available in the current EHR system, is permitted only as described in UF Health Shands Core Policies. (See CP08.003)
   c. EHR Applications with electronic signature capabilities must have the signature system reviewed and approved by UF’s Legal Services, Information Services and the Privacy Office to ensure that the electronic signature meets required standards.

3. Additions/Amendments/Corrections may only be made in health records using approved procedures; documentation should never be deleted, removed, destroyed or obliterated in primary health records.
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.2. Documentation Rules (continued)

4. **Copies of Health Records from Other Facilities/Providers**, if they were used to make healthcare decisions about the patient during treatment at UF, may be retained in any convenient, retrievable format in the patient’s primary record, whether in electronic or paper format. Relevant copies should be, but are not required to be, initialed and dated by the patient’s provider prior to adding them to the patient’s record.

5. **Record Duplications and other Errors** that cannot be corrected by individual caregivers and providers should be referred immediately to the UF Health HIM Chart Correction team. (See UF Health Shands HIM Policy ID-01)

**B. DEFINITIONS**

1. **Amendment**: The formal and deliberate addition of documentation or material to make the original documentation more complete and thereby more accurate.

2. **Authentication**: The corroboration that a person is the one claimed; most often refers to an ability to prove authorship, by written signature, initials or computer password.

3. **Availability**: The property that data or information is accessible and useable upon demand by an authorized person.

4. **Correction**: The formal and deliberate alteration, deletion or other modification of documentation to make it more accurate.

5. **Documentation**: Evidence, proof, or substantiation that certain actions were completed, information was collected, used or disclosed, or requirements were met. The act of making a record or setting down facts in permanent form.

**C. PRIVACY REQUIREMENTS**

1. **Access controls**: Technical safeguards must be implemented for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights.

2. **Person or entity authentication**: Procedures must be implemented to verify that a person or entity seeking access to electronic PHI is the one claimed.

**D. PROCEDURES**

1. **Additions/Amendments/Corrections**: Use only approved amending and error-correction procedures; never delete, remove, destroy or obliterate parts of the primary record. (See system- and facility-specific procedures.)
   a. Make “late entries” in the health record by entering the current date and time and labeling the entry as a ‘late entry’.
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.2. Documentation Rules (continued)

b. If the documentation error is on paper, make the correction by drawing a single line through the entry, writing "error" above the entry, then initialing and dating the notation. Add the correct information as close to the error as possible, or, if not possible, write “See note on (date)” near the crossed-through error and write an additional note explaining and/or correcting the error.

c. If the document was originally created in a paper format, and then scanned electronically, the imaged version must be corrected by printing the document, correcting as above (in b.), and then rescanning the document.

d. If the error is in electronic documentation, follow the error-correction procedures approved and authorized for the EHR documentation system. If needed, enter a new note, title the entry as ‘Late Entry’ or ‘Amendment,’ and document a complete explanation of any previous error with additional or corrected information.

2. Errors in Scanning Documents: If a document is imaged/scanned with a wrong encounter date or to the wrong patient, reprint the scanned document, and then rescan the document to the correct date or patient, and void the incorrectly scanned document. When in doubt, refer the issue to the UF Health HIM Chart Correction team.

3. Co-Signatures: Co-signature of a health record entry signifies acknowledgement by the co-signer that the entry was made appropriately, and implies concurrence with the statements or conclusions contained in the entry. If there is significant disagreement with the conclusion of the author, the cosigner should record such conclusions or expand on the entry as appropriate.

E. REFERENCES

1. HIPAA: 45 CFR §164.304 Definitions; §164.312 Technical Safeguards

2. Florida Statues: 456.057 Ownership and Control of Patient Records; 458.331(1)(m) Grounds for Disciplinary Action

F. EXHIBITS

None

Back to Table of Contents
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.3. Record Management Guidelines

A. POLICY

1. **Storage, Security, and Control of Active Records:** All active patient records that contain protected health information (PHI), created, received, or maintained by the University of Florida (UF) in all formats, including healthcare, financial, and research records, must be stored in physically secure areas.
   a. Paper records may not be removed from UF record storage areas or patient care areas by department or clinic staff, including faculty, fellows, and residents, without notifying the designated records manager.
   b. All electronic health information must be stored in formats and locations that meet the UF Health Information Security Standards and Policies.

2. **Removal of Patient Information from UF or Shands:** PHI, whether original or copied, in paper, electronic, or any other format, that is generated or received for the care of patients by UF, may NOT be removed from the premises by anyone, except upon receipt of a court order, a subpoena duces tecum, or written departmental administrative approval. (For instructions on how to produce records for legal depositions, see: SECTION 3: Uses and Disclosures of PHI: Health Records for Depositions in this manual.)

3. **Duplication of Patient Information:** PHI maintained in any format may not be duplicated without departmental administrative authorization, except in the following circumstances:
   a. **For Adding Document Images to Electronic Records:** Paper documents may be scanned or imaged into a patient’s electronic health record, following current imaging protocols and standards associated with the electronic record system. The original paper documents should be retained for at least 30 days and then destroyed. (See SECTION 2: HIM: Documentation Rules and SECTION 2: HIM: Retention, Archiving, and Disposal)
   b. **For Providing Copies to the Patient or Legal Representative:** Records may be photocopied or produced in hard copy or electronic format when a patient requests copies of personal health records. Only specifically authorized personnel may produce such copies. (See SECTION 4: Patient’s Rights: Access to Personal Health Records in this manual.)
   c. **For Continuity of Care:** Records/information may be duplicated when necessary to transmit health information to another health care provider, if the information is essential to ongoing treatment or services for the patient. Administrative approval must be obtained before making such copies. (See also SECTION 1: Minimum Necessary Rule in this manual.)
   d. **For Educational Purposes:** Records/information may be duplicated for educational purposes if all identifying information is removed or obliterated (patient and family names, addresses, phone numbers, e-mail addresses, clinic or department names, staff names, initials, titles, and all dates, except years). Administrative approval must still be obtained before making such copies. (See SECTION 1: Minimum Necessary Rule in this manual.)
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.3. Record Management Guidelines (continued)

e. For Legal Proceedings: Records/information may also be duplicated in preparation for legal proceedings, following UF policies and procedures. (See SECTION 3: Uses and Disclosures of PHI: Subpoenas, Court Orders, and Attorney Requests in this manual.)

4. Recovery of Lost and/or Damaged Patient Records:
   a. Reasonable efforts will be made to recover paper and electronic PHI lost due to computer malfunction, human error, misplacement, theft, water or fire damage, or any other circumstance.
   b. Unrecoverable records should be recreated as much as possible, by any methods currently available for such purposes. The fact that portions of a record were lost, unrecoverable, and have been recreated must be documented in the record with an explanation of the circumstances.

B. DEFINITIONS

1. Active/Inactive Records: Active healthcare records are those records, in all formats, currently being used for ongoing patient care, payment, litigation, or research activities. Inactive healthcare records are those for patients who have not received healthcare, made payments for care, or been involved in litigation or research for a designated period of time, but which must still be retained for a period of time prescribed by law.

2. Archiving / Storage: The act of physically or electronically moving inactive records to a storage location until the retention requirements for those records are met.

3. Patient Records: Recorded information about individually identifiable patients, including healthcare, financial, and research records, maintained in any format.

4. Primary Records: Original documentation created and maintained in any format as a direct result of a patient or client encounter in any of UF’s healthcare facilities, including faculty practice clinics and student health clinics. Paper Primary records are usually maintained in and/or by the entity where the care or service was provided.

5. Shadow Records: Paper copies of primary records that are temporarily kept separately from the primary record, usually for the convenience of health care providers or their staff. Shadow records should not be created in areas where electronic records are available.

NOTE: Paper records that were created and maintained in UF clinics are not shadow records, even though they may include documents shared with other parts of UF and with Shands.

C. PRIVACY REQUIREMENTS

Security of Active Records: All patient records in all formats must be stored so that they are physically and technologically secure, protected from unauthorized access, physical damage by fire, water, insects, pests, temperature, and humidity, and other reasonably foreseeable hazards. (See UFP Epic Policies on the UFP website, and Shands HIM Core Policies on the UF Health Shands website.)
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.3. Record Management Guidelines (continued)

D. PROCEDURES

1. General Management of Paper Records:
   a. Organize paper records to facilitate easy retrieval by authorized staff members.
      1) Keep all record documents that will not be imaged/scanned for use in electronic records inside a protective folder or binder that is clearly labeled with the patient’s name and record number.
      2) Label all pages of the record with the patient’s name and record number. Label both the front and back of pages that will be imaged/scanned for use in electronic health records.
      3) Mark folders or other binders on the outside with the year of the last episode of care, last payment, or other activity, along with pertinent patient / participant identification data.
   b. Track and account for all paper health records and individual record documents used in patient care areas.
      1) Use a sign-out process in the record file area to document the location of any record that is removed and its return.
      2) Staff members who are not directly responsible for the records should not be allowed in the paper record storage areas without supervision.
   c. Do not eat or drink when working with or near paper records to avoid damage to the documentation.

2. Removal of Other Healthcare Records: If it is necessary for faculty or staff to remove an original health record that is in a hardcopy or other tangible format (films, tapes, discs, etc.) from the record’s normal storage area, and the removal has been approved by the administrator:
   a. Sign the Record Out: Document the name of the person who has assumed responsibility for the record, where the record is being taken, and the date it was removed.
   b. Sign the Record In: Document the date of the record’s actual return.
   c. Return or Retrieve: If the record is not returned within 3 business days, contact the responsible person, and continue to follow up until it has been returned or retrieved.

3. Disaster Preparations: For potentially damaging environmental or emergency situations, initiate appropriate procedures to protect any and all records that are not stored electronically on secure servers and retrieved only through computers or similar devices, including paper records, video and audio tapes, CD’s and other portable media. Refer to UF’s Information Security Guidelines and your unit’s Information Security Manager for procedures to securely back up and/or protect electronic records. Refer to your facility’s Disaster Manual for suggested protective procedures.

4. Recovery of Lost and/or Damaged Paper Records:
   a. Lost Paper Records:
      1) Search thoroughly in all probable areas:
         a) The place where the record was last used,
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.3. Record Management Guidelines (continued)

b) The place where the record is usually filed: Look for common filing errors (transposed names or numbers) or two records filed together, etc.

c) The office of the care provider,

d) Wastebaskets and/or dumpsters.

2) Notify staff members of the loss, and allow reasonable time for a response.

3) Notify and work with the Privacy Office if there is reasonable cause to believe that:
   a) The patient may have removed the record themselves;
   b) An unauthorized person may have acquired the patient’s personal information and could use it for fraudulent purposes.

b. Fire and Water Damaged Paper Records: Prioritize the rescue of paper records using the UF Records Retention Schedules, and based on current operational needs. If the damaged records are within the retention period and there are no other copies of the records, then they must be rescued or replaced.

1) Remove records from damaged areas within 48 hours to prevent growth of mold and bacteria.

2) Restore water-damaged paper records as much as possible using available technologies:
   a) Air-Drying: Spread record pages on absorbent materials and use fans to increase airflow.
   b) Freezing: Keep records frozen or in cold storage temporarily to prevent deterioration until they can be dried out.
   c) Freeze-Drying and other recovery methods by professional document recovery specialists.

3) If it is determined that fire- or water-damaged paper records will deteriorate quickly in spite of rescue efforts, photocopy, microfilm, or digitally image them as soon as possible.

4) Create a log of the disaster event with a timeline and notes that detail the patient records affected, and the recovery efforts and results. Retain the log for the maximum retention period of the affected records.

5. When Record Recovery Is Not Possible:

a. Recreate unrecoverable records as much as possible and label each page: “Recreated Document” with the date it was recreated. Methods include:

   1) Print available documentation from (undamaged) electronic sources.
   2) Retrieve copies of previously distributed documents from recipients (shadow charts, referring physicians, other health care agencies, the patient, etc.)
   3) Request re-transcription of reports from dictation systems.

b. Document, if applicable, that portions of the record were unrecoverable in a new record as follows:

   1) Patient name and Health Record Number
   2) Types and dates of unrecovered materials, if known
   3) When and how the information was lost or destroyed
   4) Who was notified of the loss and how (include copies of notifications, if available)
   5) Signature of the record custodian or designee and date
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.3. Record Management Guidelines (continued)

6. **Subsequent Recovery of Lost Records**: If an original record that was lost or stolen is eventually recovered, merge the old and new documentation without duplication.

**E. REFERENCES:**

2. **Florida Statues**: 456.057 Ownership and Control of Patient Records

**F. EXHIBITS**

None
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.4. Retention, Archiving, and Disposal

A. POLICIES

1. **Retention**: The health record retention policies of the University of Florida (UF) are based on official schedules as well as on standards of professional practice and risk management guidelines. The subsequent death of a patient has no bearing on retention standards: Health records must be retained for the full period of time required by state laws and/or UF policies. Health records should not be retained beyond their official retention period.

   a. All primary medical records must be retained for at least ten (10) years from the date of the patient’s last episode of care, irrespective of the individual’s age or majority status at that time.

   b. Under Florida statutes, primary dental records must be retained for at least four (4) years, with certain exceptions, from the date of a patient’s last episode of care. (Refer to College of Dentistry policies for current specific retention requirements and procedures.)

   c. Other records containing PHI, including financial and research records, must be retained for the length of time prescribed in the General Records Schedule or by relevant state and federal laws.

   d. Records containing materials specifically required by HIPAA must be retained for at least six (6) years after the materials were last in effect. (Authorizations, NPP Acknowledgment forms, Disclosure Tracking Log forms, etc.)

2. **Archiving and Storage**: Primary health records and data, whether maintained in paper or electronic format, which are not being used for active provision of services, payment processes, or research may be archived until the retention requirements have been met.

   a. Only primary health, financial, and research records should be archived. The contents of true “Shadow” records should be destroyed after ascertaining that they contain only duplicates of records maintained elsewhere and do not contain any original materials.

   b. All inactive or back-up records containing PHI or other restricted data must be stored in approved storage facilities. Approved storage areas include:

      1) **On-Site**: An area inside the clinic, department, college, or other UF facility that meets the criteria listed below (C.3. Storage Areas). Record owners are responsible for making arrangements to inventory and move the records.

      2) **Off-Site**: A private professional record storage company with which UF has an active contract for services. Off-site storage arrangements for back-up electronic records must be approved by the Privacy Office.

      **NOTE**: Moving and storage warehouses, mini-storage facilities, and off-campus personal or rental property, including garages, attics, homes, mobile homes, trailers, etc., are NOT acceptable for storage of inactive records containing restricted data.

3. **Disposal and Destruction**: Record owners are responsible for arranging for safe and secure disposal of records containing PHI and other restricted data, following UF policies and the processes outlined in this policy, and using established methods which do not permit recovery, reconstruction or future use of the information.
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.4. Retention, Archiving, and Disposal (continued)

   a. Whole primary health and financial records shall only be destroyed in the ordinary course of business; no entire record shall be destroyed on an individual basis.
   b. Primary records of any type belonging to UF may only be destroyed when the retention periods established by UF have been met, and a Records Disposition Request has been approved by University Records Management.
   c. No records that are currently involved in open investigations, audits, or similar activities, or have litigation pending, shall be destroyed or otherwise discarded.

B. DEFINITIONS

1. Archiving / Storage: The act of physically moving inactive or other records to a storage location until the record retention requirements are met or until the records are needed again.
2. Destruction of Records: The routine systematic disposal of primary records to permanently remove them from active use. Destruction methods should ensure that confidentiality of the information is maintained, and that there is no possibility of reconstructing the information contained in the records.
3. Disposal of Record Documents: The day-to-day discarding of duplicate or extra reports that are not now and/or historically never were pertinent to or required for inclusion in the primary record.
4. Inactive Records: Records of patients who have not received services, made payments for services, or been involved in research for a designated period of time. Clinics and departments determine the criteria for inactive status in their areas, based on need for the records and available storage space.
5. “Scheduling” Records: Identifying types of records and then determining how long a particular type must be retained.

C. PRIVACY AND STATUTORY REQUIREMENTS

1. Chapter 257, Florida Statutes, establishes the State’s Records Management and Archives Program under the direction of the Division of Library and Information Services, Department of State, as well as specifically provides for a system for the scheduling and disposal of public records.
2. Obtaining Disposition Authorization: When records have met retention requirements, disposal of the records may be initiated by submitting a Records Disposition Request to the UF Records Management Office. The request must be submitted and approved before actual disposition is carried out. Once approved, the request form authorizes the disposition of the listed records.
3. Storage Areas for all records containing PHI or other restricted data must be physically secure and environmentally controlled, to protect the records from unauthorized access and damage or loss from temperature fluctuations, fire, water damage, pests, and other hazards.
4. Record Destruction: Primary records containing PHI or other restricted data shall only be destroyed by a bonded and insured professional document destruction company. Having a departmental or clinic representative witness the destruction is encouraged, but not required.
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.4. Retention, Archiving, and Disposal (continued)

D. PROCEDURES

1. Archiving Inactive Paper Records: Preparing records for storage
   a. **Storage Locations:** Call the Privacy Office for information about currently contracted commercial storage facilities. Transport of records is included in the services. Inventorying of records may also be arranged on the request of the record owner. Alternative arrangements for complying with security policies requiring off-site storage of back-up electronic media should be proposed in writing for approval by the Privacy Office.
   b. Preparing Primary Health Records for Storage:
      1) Create an inventory (see Forms), listing each individual record being sent to storage, so that they may be quickly retrieved, if needed. The list is also useful for documenting the destruction of the records after the retention requirement is met. The inventory list must be retained in the clinic or department that owns or is custodian for the records and should include:
         a) **Heading:** Clinic or Department name and type of record (use the current Records Schedule)
         b) **List:** Patient’s name and record number, dates of service included in each record, box number or other location indicator for each record
   2) Inventories may be in paper or electronic format.
      a) Store electronic inventories and back-up copies on a secure server or on encrypted removable media only (disk, tape, or CD), not on a workstation hard drive. Back up electronic inventories and copies regularly.
      b) Store paper inventories in a clearly labeled binder. Mark the binder: “Do Not Destroy.” Do not send the inventories to off-site storage.
   3) Remove paper health records from the active file area (shelving, file cabinets) by year and place them in approved storage boxes in the order in which they were originally filed (alphabetical or numerical).
   4) Use the storage facility’s guidelines, as appropriate, to place the boxes into storage.
   c. **Preparing Other Original/Primary Records for Storage:** Other types of records, even if they contain PHI, may, but are not required to be individually inventoried for storage. Follow steps 3) and 4) above for these records.
   d. **Shadow Records should not be archived.** Purge shadow records often and file or otherwise place any original materials in the primary records. Follow the procedure below for record disposal to permanently destroy the duplicate parts of the record. (An inventory of duplicate records disposed of in this manner is not required.)

2. Retrieving records from storage: Track the location of stored records that have been brought back to UF from storage, whether active or inactive, and adjust the storage inventory list as needed if any records are not returned to storage.

3. Disposing of Non-Primary Record Documents Containing PHI (i.e., duplicate, extra, or obsolete individual reports or data that are not and, historically, never were pertinent to the patient’s care.)
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.4. Retention, Archiving, and Disposal (continued)

a. **Controlled Destruction**: Paper records and records stored on electronic media must be immediately shredded or pulverized, electronically purged, or placed in locked or otherwise secure storage for contracted shredding/destruction. (See chart: Appropriate Record Destruction Methods at the end of this chapter.)

b. **Contracted Recycling**: Papers containing PHI may only be placed in locked bins provided under a department’s contract with a private, licensed and bonded document destruction company. Papers containing PHI may NOT be placed in any UF recycling bins for pickup by UF Physical Plant, even if the bin is locked. Papers that have already been shredded may be placed in UF recycling bins for pick-up by Physical Plant Services.

4. **Permanently Destroying Whole Health Records**

a. **Requesting Approval for Record Destruction**
   1) Complete the UF Records Disposition Request (see Forms) prior to commencing record destruction procedures. Follow the instructions included on the form.
   2) Send the Request to the address on the form. Authorization to destroy records may take 6 to 8 weeks to process.

b. **Preparing Primary Health Records for Destruction**
   1) Maintain Security: Maintain records that are scheduled for destruction in a secure location to guard against unauthorized or inappropriate access until the destruction is complete.
   2) Create an Inventory: Complete a Record Destruction Log (see Forms), individually listing each and every health record scheduled to be destroyed, or, if records are already archived, use the Storage Inventory, created when the records were put into storage, to avoid duplication of effort.
      a) Include the following information for each record (See Forms for a sample log.)
         i. Patient name and health record number
         ii. Dates of service included
         iii. Description of type of record (UF General Records Schedule type)
         iv. Date and Method of Destruction
         v. The name of the company performing the destruction
         vi. Signature(s) of individuals witnessing the destruction, if any
   b) Record Destruction Logs must be maintained for the life of the institution, and may only be maintained in paper formats.

b. **How to Destroy Patient Records**
   1) Follow the record destruction company’s protocol for carrying out the actual destruction. Do not destroy whole records within a clinic, department or unit without using a bonded, licensed record destruction company that will provide an official certificate of destruction.
SECTION 2: HEALTH INFORMATION MANAGEMENT

2.4. Retention, Archiving, and Disposal (continued)

   2) After the destruction has been completed, sign the UF Records Disposition Request and the
      Record Destruction Log.

   3) Attach the Certificate of Destruction provided by the record destruction company to the
      Disposition Request form and the Record Destruction Log.

   4) Maintain all documentation of record destruction for the life of the institution.

5. **Recovery of Inactive Records** that have been lost, stolen, or damaged: Follow the procedures outlined
   in the chapter titled *Health Information Management: Record Management Guidelines* in this manual.

### E. REFERENCES

1. **HIPAA**: 45 CFR §164.501 (Definitions); §164.502 (Use and Disclosure)

2. **Florida Statues**: 119 (Public Records – Health Records Excluded); 257 (Records Management and
   Archives Program)

### F. EXHIBITS

1. Appendix B: UF General Records Schedule

2. Appropriate Record Destruction Methods

[Back to Table of Contents]
### SECTION 2: HEALTH INFORMATION MANAGEMENT

2.4. Retention, Archiving and Disposal (continued)

#### Appropriate Record Destruction Methods

<table>
<thead>
<tr>
<th>Medium</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper Records</td>
<td>Shred (cross-cut), pulp, burn, or pulverize</td>
</tr>
<tr>
<td>Audiotapes &amp; Videotapes</td>
<td>Recycle by recording over by the original user, cut up the tapes, or pulverize/crush the tape and cassette</td>
</tr>
<tr>
<td>Computerized Data / Hard Disk Drives /</td>
<td>Professionally purge (degauss) by a certified, licensed, and bonded vendor and pulverize</td>
</tr>
<tr>
<td>Magnetic Media / Memory Sticks, Keys and</td>
<td></td>
</tr>
<tr>
<td>other USB memory devices</td>
<td></td>
</tr>
<tr>
<td>Computer Diskettes (old style: 3 and 6 inch)</td>
<td>Reformat and over-write all data, pulverize, remove from cover and cut up, or magnetically degauss</td>
</tr>
<tr>
<td>Laser Disks / Compact Disks</td>
<td>Shred or pulverize in appropriate equipment, OR break, using layers of newspaper and a hammer, OR thoroughly scratch both sides with knife or key</td>
</tr>
<tr>
<td>Microfilm / Microfiche</td>
<td>Shred or pulverize</td>
</tr>
<tr>
<td>PHI Labels on Devices, Containers, Equipment, Etc.</td>
<td>Obliterate all PHI on the label, remove and destroy the label, or incinerate the devices, container, etc., if removal or obliteration of the label is impossible.</td>
</tr>
</tbody>
</table>

[Back to Table of Contents]
SECTION 3: USES AND DISCLOSURES OF PHI

3.1. General Rules

A. POLICY

1. **General Rules for Uses and Disclosures of PHI:** The University of Florida (UF) will use and disclose protected health information (PHI) only as permitted or required by federal privacy regulations (HIPAA), other privacy-related federal laws, and relevant Florida laws. More stringent state laws will preempt HIPAA rules.

   a. Uses and disclosures that do not require a patient or representative’s written authorization are described below; all other uses and disclosures require written authorization.

   b. There are also three special circumstances in which UF is permitted to use and disclose PHI for purposes not otherwise permitted by the Privacy Rule, but only if a valid written authorization has been obtained from the individual who is the subject of the information:

      1) Most uses and disclosures of psychotherapy notes (see SECTION 3: Uses and Disclosures of PHI – “Super-Confidential” Health Information in this manual);

      2) Uses and disclosures for marketing purposes (see SECTION 3: Uses and Disclosures of PHI – Marketing in this manual.); and

      3) Uses and disclosures which meet the definition of a sale of PHI (see SECTION 3: Uses and Disclosures of PHI – Sale of PHI in this manual.)

   c. Health information and records owners at UF are responsible for maintaining a record of all disclosures of health information.

2. **Information Subject to More Stringent Laws:** Health information that is subject to specific privacy rules mandated by state or federal laws (mental health, substance abuse, STD, HIV/AIDS, genetic information) will only be used and disclosed in accordance with those laws. (See SECTION 3: Uses and Disclosures of PHI – “Super-Confidential” Health Information in this manual.)

3. **Organized Health Care Arrangement (OHCA):** UF participates in an Organized Health Care Arrangement (as defined by HIPAA) with affiliated health care providers and covered entities and will routinely disclose PHI about patients to the other participants in the arrangement for treatment, payment, and health care operations. (See SECTION 1: Health Care Components and Entities.)

4. **Disclosing PHI to other covered and non-covered entities:** UF may disclose PHI it creates, receives, and maintains to other entities outside the UF OHCA:

   a. Upon request, to a health care provider who is providing treatment to the patient;

   b. Upon written authorization by the patient or legal representative for any other purpose. (Copying fees may apply.)

5. **Minimum Necessary Rule:** Healthcare providers and staff must make every effort to reasonably limit uses, disclosures, and requests for PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. (See: SECTION 1: Minimum Necessary Rule in this manual.)
SECTION 3: USES AND DISCLOSURES OF PHI

3.1. General Rules (continued)

6. **Permitted Uses and Disclosures:** *without* the patient’s written authorization:
   a. **Internal uses for Treatment and Health Care Operations**
      (NOTE: HIPAA permits uses and disclosures of PHI for payment purposes without the patient’s written authorization; however, Florida Statutes require patient permission for such uses and disclosures; authorization is usually obtained within the Consent for Treatment.)
   b. **Disclosures to Patients and their Legal Representatives** for treatment-related purposes
      (NOTE: UF requires a written authorization for providing copies of personal health or financial records to the patient or representative for their personal use, not related to treatment.)
   c. **Limited verbal disclosures to family members and close friends** directly involved in the patient’s care or payment for care unless the patient restricts such disclosures (see **SECTION 3: Uses and Disclosures of PHI - Family Members and Friends**, in this manual).
   d. **Disclosures to Business Associates** for treatment, payment or health care operations services or assistance, when a valid Business Associate Agreement is in place.
   e. **Disclosures required for mandatory reporting** of suspected abuse or neglect.
   f. **Disclosures to vendors and technicians** for installation and maintenance of equipment, software, and other health care items that involve giving the vendor temporary access to PHI. Arrangements must be specified in the Purchase Order or contract and approved by the Chief Privacy Officer and the appropriate IT Security Officer.

7. **Other Limited Uses and Disclosures Permitted:** *without* the patient’s written authorization, if mandated and governed by other state or federal laws. Refer to your supervisor or to the Privacy Office for authorization before disclosing any information.
   a. Reporting for Public Health requirements;
   b. Reporting for Health Oversight Activities: CDC, FDA, DEA, OSHA, etc.;
   c. Responding to Subpoenas and Court Orders;
   d. Limited disclosures for certain Law Enforcement purposes;
   e. For services and processes related to decedents;
   f. For averting serious health or safety threats to the patient or others;
   g. For specialized government functions (national security, etc.);
   h. For Workers’ Compensation programs;
   i. For IRB-approved only Research Studies, using a Certificate or Waiver of Authorization.

**B. DEFINITIONS**

1. **Disclose:** To release, transfer, provide access to, or divulge in any manner, PHI held by UF.
SECTION 3: USES AND DISCLOSURES OF PHI

3.1. General Rules (continued)

2. **Health Care Operations:** Any of the following activities of the covered entity:
   a. Conducting or arranging for Quality Assessment and Improvement activities, health care reviews, legal services, and auditing functions, including fraud/abuse detection and compliance programs;
   b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs, accreditation, certification, licensing, or credentialing activities;
   c. Business planning and development, and business management and general administrative activities of the entity. (See *Appendix A: Glossary* for full definition.)

3. **Payment:** Activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care. (See *Appendix A: Glossary* for full definition.)

4. **Professional Need to Know:** A required level of access to specific and limited information necessary to complete assigned work.

5. **Super-Confidential Information:** Information pertaining to Substance Abuse, Mental Health Conditions, HIV Testing, Sexually Transmitted Diseases, and Genetic Information, as defined and protected by specific federal and state laws and regulations.

6. **Treatment:** The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one provider to another.

7. **Use:** To employ, apply, utilize, share, examine, or analyze PHI held by UF.

### C. PRIVACY REQUIREMENTS

1. **Standard:** A covered entity or business associate may not use or disclose PHI, except as permitted or required by the Privacy Rule.

2. **Permitted uses and disclosures:** A covered entity is permitted to use or disclose PHI as follows:
   a. To the individual;
   b. For treatment, payment, or health care operations, as permitted by the Privacy Rule;
   c. Incident to a use or disclosure otherwise permitted or required by the Privacy Rule, provided that the covered entity has complied with the minimum necessary requirements;
   d. Pursuant to and in compliance with a valid authorization (except for uses and disclosures of genetic information that are prohibited for underwriting purposes);
   e. Pursuant to an agreement or as otherwise permitted for uses and disclosures requiring an opportunity for the individual to agree or to object; and

3. **Required disclosures:** A covered entity is required to disclose PHI:
   a. To an individual, when requested, or otherwise required by, the Privacy Rule; and
SECTION 3: USES AND DISCLOSURES OF PHI

3.1. General Rules (continued)

b. When required by the Secretary (of HHS) to investigate or determine the covered entity’s compliance with HIPAA.

4. Accounting for disclosures: An individual has a right to receive an accounting of disclosures of PHI made by a covered entity. (See SECTION 4: Patient’s Rights – Accounting For Disclosures in this manual.)

D. PROCEDURES


2. For use of patient records for depositions, see SECTION 3: Uses and Disclosures of PHI: Records for Depositions in this manual.

3. For disclosures in response to subpoenas, court orders, and attorney requests, see SECTION 3: Uses and Disclosures of PHI: Subpoenas, Court Orders and Attorney Requests in this manual.

4. For disclosures of “Super-Confidential” Health Information, also follow the special-handling procedure in SECTION 3: Uses and Disclosures – “Super-Confidential” Health Information in this manual, in addition to the procedures below.

5. Responding to Requests for copies of PHI – General Rules: After receiving a valid authorization, subpoena, court order, or a patient request that does not require an authorization, process the request for copies of records as follows:

   a. Even though 30 days are available to respond to requests for records, respond within 10 business days of receipt of the request, whenever possible. If unable to respond within the first 10 days, notify the requestor of the reason for the delay and progress of the request. If unable to respond within 30 days, notify the Privacy Office immediately.

   b. For paper records (only): Number each original page to be copied; number front and back of pages with documentation on both sides, counting each side as a separate page.

   c. For copies not related to treatment, calculate the fee to be charged from the table below; each copied side of a paper document counts as one page. Notify the requestor of the amount of the fee, and wait for a response before beginning to copy the record.

   d. Provide copies in the format requested by the patient, if possible: photocopy, print out, scan, or otherwise duplicate only the portions of the record specifically requested. If copies are reproduced onto electronic media, encrypt the media.

   e. Create and attach a cover letter, including the patient’s name and record number, the names of the reports/documents copied, the number of pages/documents copied, the date-range of the materials, and the amount charged and paid.
SECTION 3: USES AND DISCLOSURES OF PHI

3.1. General Rules (continued)

f. File or scan the patient’s authorization or letter of request, the subpoena, court order, or attorney request with authorization, a copy of the cover letter, a copy of the certification (if one was provided), and any return mail receipts into the patient’s record.

g. If the request is also for a patient’s billing records, fax/scan a copy of the request to the Patient Services & Accounting Department so they can send the patient’s billing records to the requestor.

6. Record and Describe All Disclosures of Health Information:
   a. In addition to placing or scanning all request-related documents into the patient’s record, also record the disclosure in a permanent log and retain the log in the clinic or department. The log may be maintained manually, on paper, or electronically, in a secure computer database, and should include:
      1) The patient’s name and health record number
      2) The date the request was received
      3) The name and address of the requestor
      4) The purpose of the request
      5) A list of the reports that were disclosed and the date of disclosure, or the disposition of the request, if no information was disclosed.
   b. Clinics and departments using an outside copying service may rely on the disclosure log maintained by the company and left with the department/clinic after each visit.

7. For non-authorized disclosures that were not related to treatment or health care operations, enter the appropriate information in UF’s online Disclosure Tracking System. (See SECTION 4: Patient Rights: Accounting for Disclosures in this manual for more information and instructions.)

8. New Products Using Electronic PHI: When purchasing, developing, upgrading, or enhancing a product or system that involves storing electronic PHI in new locations, using new technology, sharing PHI with outside entities, or potential or actual access to PHI in any format by researchers, vendors, installation, and maintenance technicians, or other persons who are not part of UF’s workforce:
   a. Refer to the Information System Security Evaluation developed by HSC IT Security. Complete the current Security Checklist with your Information Security Manager and the vendor or developer of the new software or system.
   b. If PHI will be accessed or used by the vendor or technicians in the new system, establish a Business Associate Agreement with the vendor. (See HIPAA: Organizational Requirements: Business Associates and Vendors in the HIPAA Privacy Management manual.)
   c. Receive approval from both the Privacy Office and the Information Security Team for the new software or system prior to beginning installation or upgrades.
SECTION 3: USES AND DISCLOSURES OF PHI

3.1. General Rules (continued)

9. **Responding to Agencies that Claim Exemption from HIPAA Privacy Regulations:** Agencies and entities such as the American Red Cross, WIC, law enforcement, and schools may claim exemption from the requirements of federal and state privacy laws. However, the health care components of UF are not exempt from HIPAA. Do not disclose PHI from UF to third parties without specific written authorization from the patient or representative or a legally issued subpoena or court order. Refer all such requests to the Privacy Office, if necessary.

10. **Responding to Media Requests for Patient Information:** Direct any requests from journalists and news entities for information concerning a patient’s condition (when the patient is currently undergoing treatment) to the UF Health News and Communications Department during general business hours and to the University Police Department for referral after normal business hours.

**E. REFERENCES:**

HIPAA: 45 CFR §160.103 Definitions; §164.501 Definitions; §164.502 Uses and Disclosures: General Rules; §164.506 Uses and Disclosures to carry out treatment, payment, or health care operations; §164.508 Uses and disclosures for which an authorization is required; §164.514(f) Other Requirements

**F. EXHIBITS:**

None

[Back to Table of Contents]
SECTION 3: USES AND DISCLOSURES OF PHI

3.2. “Super-Confidential” Health Information

A. POLICY

NEW: 09/01/2013

1. Protected by Law: Health information that is subject to specific privacy rules (mental health, substance abuse, genetic information, HIV/AIDS, sexually transmissible diseases), which are mandated by state or federal laws that are more stringent than HIPAA, will only be used and disclosed in accordance with those more stringent laws.

2. Limited Disclosures: In general, “super-confidential” health information shall not be released or made public by anyone, except under the following circumstances:
   a. With the consent of the person(s) to which the information applies;
   b. For statistical and research purposes, as long as the information is summarized so that no person can be identified and no names are revealed;
   c. To healthcare personnel, appropriate state agencies, public health agencies, or courts of appropriate jurisdiction, to enforce any applicable laws;
   d. In a medical emergency, but only to the extent necessary to protect the health or life of a named party, or an injured officer, firefighter, paramedic, or emergency medical technician; or
   e. To the proper authorities as required by other applicable laws.

B. DEFINITIONS

1. Disclose: To release, transfer, provide access to, or divulge in any manner, PHI held by UF.

2. Genetic Information means:
   a. With respect to an individual, information about:
      1) The individual’s genetic tests;
      2) The genetic tests of family members of the individual;
      3) The manifestation of a disease or disorder in family members of such individual; or
      4) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.
   b. Concerning an individual or family member of an individual, the genetic information of:
      1) A fetus carried by the individual or family member who is a pregnant woman; and
      2) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.
   c. Genetic information excludes information about the sex or age of any individual.

3. Genetic Services: A genetic test; genetic counseling (including obtaining, interpreting, or assessing genetic information); or genetic education.
SECTION 3: USES AND DISCLOSURES OF PHI

3.2. “Super-Confidential” Health Information (continued)

4. Genetic Test: an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

Psychotherapy Notes: Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record.

“Psychotherapy notes” excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

5. Super-Confidential Information: Information pertaining to Substance Abuse, Mental Health Conditions, HIV Testing, Sexually Transmissible Diseases, and Genetic Information, as defined and protected by specific federal and state laws and regulations.

6. Use: To employ, apply, utilize, share, examine, or analyze PHI held by UF.

C. PRIVACY REQUIREMENTS

1. Sexually Transmissible Diseases: (F.S. 384.29)
   a. All information and records held by the [Department of Health] or its authorized representatives relating to known or suspected cases of sexually transmissible diseases are strictly confidential and exempt from the provisions of s. 119.07(1).
   b. Such information shall not be released or made public by the department [DOH] or its authorized representatives, or by a court or parties to a lawsuit upon revelation by subpoena, except under the circumstances enumerated in the statute.
   c. When disclosure is made pursuant to a subpoena, the court shall seal such information from further disclosure, except as deemed necessary by the court to reach a decision, unless otherwise agreed to by all parties.

2. Human Immunodeficiency virus testing: (F.S. 381.004) The identity of a person upon whom a test has been performed and test results are confidential and exempt from the provisions of s. 119.07(1).

Penalties: Any person who obtains information that identifies an individual who has a sexually transmissible disease including human immunodeficiency virus or acquired immunodeficiency syndrome, who knew or should have known the nature of the information and maliciously, or for monetary gain, disseminates this information or otherwise makes this information known to any other person, except by providing it either to a physician or nurse employed by the department or to a law enforcement agency, commits a felony of the third degree.
SECTION 3: USES AND DISCLOSURES OF PHI

3.2. “Super-Confidential” Health Information (continued)

3. **Mental Health:** (F.S. 394.4615) A clinical [mental health] record is confidential and exempt from the provisions of s. 119.07(1). Unless waived by express and informed consent, by the patient or the patient’s guardian or guardian advocate or, if the patient is deceased, by the patient’s personal representative or the family member who stands next in line of intestate succession, the confidential status of the clinical record shall not be lost by either authorized or unauthorized disclosure to any person, organization, or agency.

4. **Psychotherapy notes:** (HIPAA) A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:
   a. To carry out the following treatment, payment, or health care operations:
      1) Use by the originator of the psychotherapy notes for treatment;
      2) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
      3) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and
   b. A use or disclosure that is:
      1) Required by the Secretary (of HHS) to investigate or determine the covered entity’s compliance with HIPAA,
      2) Required by law,
      3) Permitted by health oversight activities, with respect to the oversight of the originator of the psychotherapy notes,
      4) Permitted for coroners and medical examiners to perform their duties, or
      5) In situations where the covered entity, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to health or safety.

5. **Substance Abuse:** (F.S. 397.501) The records of service providers which pertain to the identity, diagnosis, and prognosis of and service provision to any individual are confidential in accordance with this chapter and with applicable federal confidentiality regulations and are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

(42 CFR 290dd-3/290ee-3) Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any alcohol/drug abuse prevention function conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall be confidential and be disclosed only for the purposes and under the circumstances expressly authorized under [this federal rule].

6. **Genetic Testing:** (F.S. 760.40) DNA analysis may be performed only with the informed consent of the person to be tested, and the results of such DNA analysis, whether held by a public or private entity, are the exclusive property of the person tested, are confidential, and may not be disclosed without the consent of the person tested. (Exceptions apply; see the statute.)
SECTION 3: USES AND DISCLOSURES OF PHI

3.2. “Super-Confidential” Health Information (continued)

**D. PROCEDURES:**

1. Responding to requests for Super-Confidential Health Information:
   a. By Authorization from the Patient or Legal Representative:
      1) Verify that the authorization includes necessary specific permissions for the super-confidential
         health information to complete the request. For example, if the record contains mental health
         information, the authorization must specifically include release of mental health records.
      2) If the authorization is incomplete or non-specific for the super-confidential health information,
         contact the patient or the patient’s legal representative and verify that he/she is aware of the
         contents of the record and whether the patient/representative’s specific permission will be
         granted to release the requested information.
         a) With the patient’s permission, notify the requesting entity that the authorization does not
            meet requirements and request a more specific authorization; or
         b) Provide a copy of UF’s Authorization form directly to the patient.
      3) When a valid authorization is obtained, process the health records according to the established
         procedure, and stamp the pages as appropriate (see below).
   b. By Subpoena or Court Order:
      1) Subpoenas:
         a) Health Information concerning sexually transmissible, excluding HIV/AIDS information, may
            be released in response to a subpoena alone. Follow the procedures for responding to
            subpoenas (SECTION 3: Uses and Disclosures of PHI – Subpoenas, Court Orders, Attorney
            Requests in this manual).
         b) Health information concerning substance abuse treatment, mental health, and HIV/AIDS
            testing may NOT be released in response to a subpoena alone. The patient or the patient’s
            legal representative must also provide a signed authorization, specifically allowing the
            release of the requested information.
            i. Contact the patient or legal representative directly and request an authorization for the
               release of the information.
               **Note:** It is extremely important to contact the patient/representative directly to avoid
               disclosing the patient’s super-confidential health information to the patient’s attorney
               or to the opposing attorney, in case this information has not already been disclosed.
            ii. Process the records according to the established procedure, and stamp the pages with
                the appropriate non-redisclosure statement (see below).
      2) Court Orders: Refer all court orders for the release of health information to the UF AHC
         General Counsel’s Office.
SECTION 3: USES AND DISCLOSURES OF PHI

3.2. “Super-Confidential” Health Information (continued)

2. **Required Non-Redisclosure Statements**: stamp the appropriate statement (following) on each copied page, as required by federal and state laws.

   a. **Alcohol/Drug Abuse Records** from federally assisted drug/alcohol rehabilitation programs, Federal Law 42 CFR, Part 2.32: “This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR, part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains, or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for the purpose. The Federal rules restrict any use of this information to criminally investigate or prosecute any alcohol or drug abuse patient.”

   b. **HIV/AIDS Testing and Results** (F.S. 381.004(2)(f)): “This information has been disclosed to you from records whose confidentiality has been protected by state law. State law prohibits you from making any further disclosure of such information without the specific consent of the person to whom such information pertains or as otherwise permitted by state law. A general authorization for this release of health or other information is NOT sufficient for this purpose.”

3. **Non-Redisclosure Statement for Mental Health Records**: This requirement is no longer included in the Florida Statutes, but has been retained by UF as a suggested standard of practice. Stamp copies with: “Confidential and Privileged Information for Professional Use Only”

**E. REFERENCES:**

1. **HIPAA**: 45 CFR §160.103 Definitions; §164.508(b)(1) Authorizations

2. **Title 42: Public Health – Part 2, Subpart A** - § 2.1 and § 2.2: Confidentiality of Alcohol and Drug Abuse Patient Records

3. **Florida Statutes**: 381.004(3) – HIV testing – Confidentiality; 384.29 – Sexually Transmissible Diseases – Confidentiality; 394.4615 – Mental Health – Clinical records: Confidentiality; 397.501 – Substance Abuse – Rights of individuals: Confidentiality; 456.057(12) – Record Disclosures; 760.40 – Genetic Testing: Confidentiality

**F. EXHIBITS:**

None
SECTION 3: USES AND DISCLOSURES OF PHI

3.3. Family Members and Friends

A. POLICY

1. **Use and Disclosure:** The University of Florida (UF) may, but is not required to, disclose limited, relevant, protected health information (PHI), without the patient’s written authorization, to a family member or friend who has been specifically identified by the patient or who is directly involved in the care of the patient or the payment for care. Patients may also authorize disclosures of health information to specific family members or friends at any time, either verbally or in writing.

2. **Scope of Policy:**
   a. This policy pertains specifically to patients as they are being seen for care in UF medical, dental, and nursing clinics and departments, the Student Health Care Center, and the UF Counseling and Wellness Center. It does not apply to patients being seen as inpatients in Shands; for those circumstances, care givers should follow relevant Shands policies.
   b. This policy pertains to limited verbal disclosures of PHI to persons directly involved in a patient’s treatment, for purposes of notifying such persons of a patient’s current location, general condition, or death, as specified in the Privacy Rule. It also applies to limited disclosures of PHI, which may be in printed, e-mail, or other written formats, to such persons for the purposes of making appointments, receiving appointment reminders, and making billing or payment inquiries on behalf of a patient.
   c. This policy does not apply to disclosures of health care information unrelated to the patient’s current condition, nor does it apply to the provision of copies of health records; in both cases, a written authorization must be provided by the patient or the patient’s legal representative.

3. **Application:** This policy applies in situations where the patient is present and able to make decisions as well as situations where the patient is not present and/or cannot give permission. In either case, the health care provider may share or discuss only the information that the person involved needs to know about the patient’s care or payment for care.
   a. If the patient is present and able to make decisions, reasonable efforts will be made to inform the patient in advance and allow the patient the opportunity to object to the disclosure.
      1) In most cases, the Notice of Privacy Practices will serve as notification to patients of their right to object to disclosures of their PHI to family members or friends, as described in this policy.
      2) The patient may also be informed, and consent obtained, verbally.
   b. If the patient is not present and/or cannot give permission, the patient’s health care provider must use professional judgment to determine if sharing the patient’s PHI with family, friends, or others is in the patient’s best interest. When someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient has asked the person to be involved in the care or payment for care.
SECTION 3: USES AND DISCLOSURES OF PHI

3.3. Family Members and Friends (continued)

4. **Expectations:** Providers and staff are expected to only disclose PHI when acting within, and as the information relates to, the scope of their assigned duties. However, there may also be occasions where staff must use professional judgment when disclosing patient information, taking into consideration the patient’s best interests as well as the patient’s right to privacy.

### B. DEFINITIONS

1. **Disclose:** To release, transfer, provide access to, or divulge in any manner, PHI held by UF.

2. **Family Member**, with respect to an individual:
   a. A dependent (as such term is defined in 45 CFR 144.103), of the individual; or
   b. Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).
      1) First-degree relatives include parents, spouses, siblings, and children.
      2) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.
      3) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
      4) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

3. **Personal Representative:** A person acting on behalf of the patient who must be treated as the patient for the purposes of the privacy regulations. (See **SECTION 1: General HIPAA and Privacy Rules: Verification of Identity and Authority** in this manual for a list of appropriate personal representatives.)

### C. PRIVACY REQUIREMENTS

1. **Uses and disclosures requiring an opportunity for the individual to agree or to object, specifically, involvement in the individual’s care and notification purposes:** A covered entity may disclose to a family member or other relative, a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person’s involvement with the individual’s health care or payment related to the individual’s health care.
   a. **Uses and disclosures with the individual present:** If the individual is present for, or otherwise available, prior to a permitted use or disclosure and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:
      1) Obtains the individual’s agreement;
      2) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
SECTION 3: USES AND DISCLOSURES OF PHI

3.3. Family Members and Friends (continued)

3) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

b. **Limited uses and disclosures when the individual is not present:** If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual’s incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person’s involvement with the individual’s care or payment for care, or needed for notification purposes. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual’s best interest in allowing a person to act on the individual’s behalf to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

c. **Uses and disclosures when the individual is deceased:** If the individual is deceased, a covered entity may disclose to a family member, or other persons identified above who were involved in the individual’s care or payment for health care prior to the individual’s death, PHI of the individual that is relevant to such person’s involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

2. **Purpose of Disclosure:** A covered entity may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual’s location, general condition, or death.

**D. PROCEDURES:**

1. **Make reasonable efforts to verify** the identity of any person requesting information about, or acting on behalf of the patient, prior to discussing the patient’s PHI with them. Ask the person to describe their relationship to the patient and their authority or need to receive the patient’s information. (See **SECTION 1: Verification of Identity and Authority** in this manual.)

   a. After a family member or friend’s identification and direct involvement in the patient’s care has been satisfactorily verified, the patient’s PHI, limited to whatever is directly relevant to the person’s involvement with the patient’s care or payment for care, may be discussed face to face, over the phone, or in writing with the verified person.

   b. Providers and staff may also reasonably rely on prior experiences, if a family member or friend is known by providers and staff and there is a history of information being shared with this person during past encounters, unless there is knowledge that the patient’s relationship with this person has changed.

   c. If a parent or legal guardian of a minor child or vulnerable adult (the patient) requests to establish a written list of people with whom health information may not be discussed, such requests may be accommodated within reason and at the clinic’s discretion. The list should also provide a method for reliably identifying the “restricted” individuals.
SECTION 3: USES AND DISCLOSURES OF PHI

3.3. Family Members and Friends (continued)

2. **Authorizations:** If the patient has authorized, verbally or in writing, limited verbal or written disclosures of PHI to another person:
   a. Document verbal authorizations in the patient’s health record, preferably with a signed authorization from the patient; review any ongoing agreements with the patient periodically and update any changes.
   b. When using written authorizations, check the expiration date and for any other specified limitations prior to disclosing information to the authorized person. (See SECTION 3: Uses and Disclosures – Authorizations in this manual for more information.)

3. **Unique Identifier or Password:** If appropriate, establish a method for uniquely identifying the family member or friend for use in telephone verification, such as a password, unique number identifier, or other agreed-upon indicator.

4. **Minimum Necessary Applies:** Use the “minimum necessary rule,” standard reasonable precautions, and professional judgment at all times to protect the patient’s privacy rights.

**E. REFERENCES:**

**HIPAA:** 45 CFR §160.103 Definitions; §164.510(b) Uses and Disclosures – for involvement in the individual’s care and notification purposes

**F. EXHIBITS:**

None

[Back to Table of Contents]
SECTION 3: USES AND DISCLOSURES OF PHI

3.4. Authorizations for Release of Health Information

A. POLICY

1. **Uses and Disclosures of PHI must always be authorized:** The University of Florida (UF) may use or disclose protected health information (PHI) only if authorized by the patient or the patient’s personal representative, or by applicable laws which permit uses and disclosures without the patient’s specific authorization.

2. **Verification:** UF will make reasonable efforts to verify the identity of any person authorizing a use or disclosure of PHI. If the authorizing person is not the patient, UF will also make reasonable efforts to verify the person’s relationship to the patient and their authority to consent to the use or disclosure. (See SECTION 1: Verification of Identity and Authority in this manual.)

3. **Valid Authorizations:** Authorizations for release of health information must be in writing and may be delivered to UF by mail, fax, or in person. Signed documents and forms may also be scanned and e-mailed to the appropriate record custodian.
   a. Official UF authorization forms that have any of the following defects will not be valid for use or disclosure of PHI under any circumstances:
      1) Incomplete in any part,
      2) Are known to have expired,
      3) Are known to have been revoked, or
      4) Appear falsified in any way.
   b. Written requests for release of health information that are not on official UF or other forms will be evaluated case by case; if honored, such requests will only be valid for one release of health information. A completed form will be required for subsequent releases of information.

4. **Revoking an Authorization:** An individual may revoke an authorization at any time, as long as the revocation is in writing. The revocation will be effective immediately when received, except to the extent that UF has already disclosed information in reliance upon the authorization. Once received and processed, no further information will be disclosed.

5. **Use of Forms:** UF’s official authorization forms are preferred, but not exclusively required, as long as the forms provided (for example, from other facilities, insurance companies, or attorneys) include all the required elements and statements described under Privacy Requirements below.

6. **Expiration Date:** Authorizations are generally only valid for disclosing information created prior to the date the authorization was signed. If the authorization includes a statement that information created after the date of signing may be included in future disclosures, then information created up to the expiration date may also be disclosed.

7. **Alteration or modification** of UF authorization forms by UF healthcare components is not allowed except by special permission and approval of the Privacy Office.
SECTION 3: USES AND DISCLOSURES OF PHI

3.4. Authorizations for Release of Health Information (continued)

8. **Retention:** UF must retain all authorizations it acts upon for the applicable retention period required by federal or state laws.

9. **Verbal Agreements/Authorizations,** when allowed, may be documented in a patient’s health record by health care personnel. Verbal authorizations are usually time-limited and only valid for the immediate purpose for which the agreement was given by the patient or representative.

**B. DEFINITIONS**

1. **Authorization:** A document or the action or fact of giving consent or permission or conferring authority on another person or entity.

2. **Disclose or Disclosure:** The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

3. **Expiration Date:** The date through which an authorization may be used to disclose health information created prior to the date the authorization was signed. For example: On 8/1/13, an attorney presents an authorization signed by her client on 2/12/12. The expiration date on the authorization is 2/12/14, which means it is still valid, but only for information that was created prior to 2/12/2012. If any information was created after that date, a new authorization is needed for its release.

4. **Personal Representative:** A person acting on behalf of the patient who must be treated as the patient for the purposes of the privacy regulations. (See SECTION 1: Verification of Identity and Authority for a list of appropriate personal representatives.)

**C. PRIVACY REQUIREMENTS**

1. **Authorization required: general rule:** Except as otherwise permitted or required by the Privacy Rule, a covered entity may not use or disclose PHI without an authorization that is valid. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

2. **A valid authorization** is a document that meets the following requirements:
   
   a. Includes six core elements required by the Privacy Rule:
      
      1) Specific, meaningful description of the information to be disclosed;
      2) The name of the entity authorized to make the disclosure;
      3) The name of the entity to whom the information may be disclosed;
      4) A description of the purpose of the disclosure;
      5) An expiration date or event;
      6) The signature of the patient or personal representative and the date of signing.

   b. Includes three statements required by the Privacy Rule:
      
      1) The patient’s right to revoke the authorization in writing, the exceptions to this right, and a description of how to revoke;
SECTION 3: USES AND DISCLOSURES OF PHI

3.4. Authorizations for Release of Health Information (continued)

2) The ability or inability to condition treatment, payment, or eligibility for benefits on the authorization; and

3) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer protected by the privacy regulations.

c. The authorization must be written in plain language.

3. **Provision of Copies**: UF must provide the individual with a copy of any authorization signed at the UF’s request.

D. **PROCEDURES**:

1. **Verify Identity and Authority**: Make reasonable efforts to verify the identity of a person presenting an authorization for release of health information, and if not the patient, their relationship to the patient and authority to sign the authorization. (See **SECTION 1: Verification of Identity and Authority** in this manual.) If a patient or legal representative has documents to corroborate identity or authority, attach copies to the form.

2. **Use the correct form**: Whenever possible, use forms that are applicable to the situation: Forms are available for general use, marketing, fundraising, research, e-mail and other electronic communications, sale of PHI, publications, and public relations. (See the specific sections in this manual for more information and instructions.)

3. **Provide assistance**: Assist the patient or representative to complete an Authorization form as needed. Give the requestor a copy of the completed form.

4. **Return incomplete or invalid authorizations** to the requestor with an explanation of the defect and how to correct it. Wait until a valid authorization is received before proceeding with any disclosures.

5. **Forward completed authorizations** to the person or department responsible for the release of the information requested. If using a record copying service, forward the authorization to the service representative. (See also **SECTION 3: Uses and Disclosures of PHI: Subpoenas, Court Orders, and Attorney Requests**.)

E. **REFERENCES**

**HIPAA**: 45 CFR §164.508 Uses and disclosures for which an authorization is required.

F. **EXHIBITS**

Authorization to Use and Disclose PHI

[Back to Table of Contents]
SECTION 3: USES AND DISCLOSURES OF PHI

3.5. Health Records for Depositions

**A. POLICY**

NEW 07/01/2012

1. **Using and Disclosing Health Records for Depositions:** Health records, in paper, electronic or any other format, are the property of the University of Florida (UF) and not of any individual staff member. Original records and copies of records may only be removed from the premises by an authorized record custodian under a lawfully issued subpoena or court order. Records may not be removed from UF or Shands facilities in any format by individuals responding to a subpoena, which has been served on the individual for a deposition, with or without an order for production of records.

   a. UF personnel called for depositions may not take original health records or copies of records with them for use during a deposition.

   **Note:** Per the General Counsel’s Office: Individuals being subpoenaed for deposition must not bring anything to the deposition, especially anything that wasn’t previously requested via a valid subpoena. Anything he or she brings to the deposition and relies upon to respond to the questions may be viewed by the deposing attorney.

   b. Health records required for a deposition must be subpoenaed by the attorney or ordered by the court separately when production of the record is necessary.

2. **Disclosures:** Only authorized record custodians may copy and provide UF health information in response to court orders, subpoenas, and other lawful processes, following UF’s privacy and other policies for this purpose. (See **SECTION 3: Uses and Disclosures of PHI: Subpoenas, Court Orders, and Attorney Requests** in this manual.)

**B. DEFINITIONS**

1. **Deposition:** The testimony of a party or witness in a civil or criminal proceeding taken before trial, usually in an attorney's office or other location convenient to all parties.

2. **Lawfully Issued Subpoena:** a subpoena issued by or under the jurisdiction of a Florida or federal court. Subpoenas issued by other state courts will not be honored.

**C. PRIVACY REQUIREMENTS**

1. **Disclosures for judicial and administrative proceedings:** A covered entity may disclose PHI in the course of any judicial or administrative proceeding: (i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the PHI expressly authorized by such order; or (ii) In response to a subpoena, discovery request, or other lawful process.

2. **Pre-emption:** The provisions of the Privacy Rule do not supersede other provisions of the federal privacy regulations or other state laws that otherwise permit or restrict uses or disclosures of PHI.
D. PROCEDURES

1. If a subpoena for a deposition is served to a UF staff member, the individual should inform the deposing attorney prior to the deposition that the person being deposed is not the official custodian for the records and will not be able to bring the requested records, either originals or copies, to the deposition.

2. Assist the attorney to determine if Shands or UF is the official record custodian that must be served with a valid subpoena or court order so that the records will be available for the deposition. See SECTION 2: Health Information Management: Record Custodians List in this manual.

3. Contact the HSC Office of General Counsel for other assistance with depositions and subpoenas.

E. REFERENCES

HIPAA: 45 CFR §164.512(e) Disclosures for Judicial and Administrative Proceedings

F. EXHIBITS

None
SECTION 3: USES AND DISCLOSURES OF PHI

3.6. Subpoenas, Court Orders, Attorney Requests

A. POLICY

1. Disclosures: Health record custodians for the University of Florida (UF) may disclose protected health information (PHI) for judicial and administrative proceedings in response to: an order of a court or administrative tribunal, or a lawfully issued subpoena, discovery request, or other lawful process, in accordance with all applicable laws and regulations.

2. Individual UF providers who receive a subpoena for production of health records may not provide copies of records as they are generally not the record custodian, but rather should immediately turn subpoenas over to the UF clinic or unit where the patient was seen, or to Shands Health Information Management.

3. Information Subject to More Stringent Laws: Health information that is subject to privacy rules under specific state or federal laws (substance abuse, mental health, STD, HIV, genetic, etc.) will only be disclosed in accordance with those laws.

4. Fees: UF will charge a reasonable fee, as allowed by state and federal laws, for copies of records.

B. DEFINITIONS

1. Lawfully Issued Subpoena: A subpoena issued by or under the jurisdiction of a Florida or federal court. Subpoenas issued by other state courts will not be honored.

2. Qualified Protective Order: An order of a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
   a. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
   b. Requires the return to the covered entity or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

3. Satisfactory Assurance: A written statement and accompanying documentation demonstrating that the patient was made aware of the disclosure and any objections have been satisfactorily resolved. (See Disclosures for Judicial and Administrative Proceedings in the HIPAA Privacy Management manual for more details.)

4. Super-Confidential Information: Information pertaining to Substance Abuse, Mental Health Conditions, HIV Testing, HIV/AIDS, Sexually Transmitted Diseases, and Genetic Information, as defined and protected by specific federal and state laws and regulations.

C. PRIVACY REQUIREMENTS

1. Disclosures for judicial and administrative proceedings: A covered entity may disclose PHI in the course of any judicial or administrative proceeding:
SECTION 3: USES AND DISCLOSURES OF PHI

3.6. Subpoenas, Court Orders, Attorney Requests (continued)

a. In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the PHI expressly authorized by such order; or

b. In response to a subpoena, discovery request, or other lawful process, if:
   1) The covered entity receives satisfactory assurance (see definition above) from the party seeking the information that reasonable efforts have been made to ensure that the individual who is the subject of the PHI has been given notice of the request; or
   2) The covered entity receives satisfactory assurance (see definition above) from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order.

2. Pre-emption: The provisions of the Privacy Rule do not supersede other provisions of the federal privacy regulations or other state laws that otherwise permit or restrict uses or disclosures of PHI.

D. PROCEDURES

1. Processing Requests for Health Records for Judicial Purposes: Gainesville or Jacksonville

   a. When Shands is the Custodian: If Shands is the custodian for a clinic’s primary records, that clinic should forward subpoenas, court orders, and attorney requests for health information to the Shands Health Information Management Department (HIM). (See SECTION 2: Health Information Management: Record Custodians List in this manual.)
      1) Never use “shadow records” to respond to subpoenas, court orders, or attorney requests.
      2) Forward any original materials in relevant shadow charts to HIM with the subpoena or request.
      3) HIM Release of Information specialists will ensure that all requested components (clinical and financial) that can legally be disclosed are included in the response.

   b. When UF is the Custodian and is using Contracted Copying Services: If the clinic or department holds the primary records being requested, and has a contract with a record copying service, forward all subpoenas, court orders, and attorney requests for disclosure of PHI to the copying service representative. The representative will assure that all requested components (clinical and financial) that can legally be disclosed are included in the response.

   c. When UF is the Custodian, but is not using Contracted Copying Services: If the clinic or department holds the primary health records being requested, but does not use a record copying service, fax or e-mail a copy of all subpoenas, court orders, and attorney requests for disclosure of health information (only) to either the Gainesville or Jacksonville Privacy Office, as appropriate, to obtain permission to disclose the requested information. Do not send original documents.
      1) If the request is determined to be valid, the Privacy Office will notify the clinic or department so that the request for records may be processed.
      2) If there are deficiencies in the request, court order, subpoena or accompanying documentation, the Privacy Office will communicate with the record manager in the clinic or department or with the person or entity requesting the information. Once the problem is corrected, the clinic or department will be notified so that the records may be processed.
SECTION 3: USES AND DISCLOSURES OF PHI

3.6. Subpoenas, Court Orders, Attorney Requests (continued)

3) Process the record following the procedure in SECTION 3: Uses and Disclosures of PHI: General Rules.

4) If the requested records include information related to substance abuse, mental health, HIV/AIDS, sexually transmissible diseases, or genetic information, see the response process for Super Confidential Records, SECTION 3: Uses and Disclosures: “Super-Confidential” Health Information.

2. All other subpoenas or public records requests: Contact the Health Science Center Office of General Counsel for assistance.

3. Certification of Authenticity: If certification of copied/duplicated documents is requested:
   a. Record custodians and their delegates are authorized to complete and sign UF’s Certification of Authenticity form (See Forms), when needed. Have the completed form notarized. Do not complete certification forms supplied by the persons or entities requesting the records without consulting with the Privacy Office.
   b. Certification forms are not stand-alone documents; they must be attached to or otherwise included in the paper or electronic copies being certified. Do not certify copies of records after they have been provided to the requestor.
   c. Deliver copies to the individual who requested the records:
      1) Send paper copies or electronic media/discs via First Class Mail, Return Receipt Requested (send any required encryption key separately); or
      2) Deliver paper copies or electronic media/discs (along with any required encryption key) in person; request a signed copy of your cover letter as a receipt for the delivery.

E. REFERENCES

HIPAA: 45 CFR §164.512 (e) Disclosures for Judicial and Administrative Proceedings

F. EXHIBITS:

Copying, Production, and Inspection Fees

<table>
<thead>
<tr>
<th>Services</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspection of Records: Per hour</td>
<td>$25.00</td>
</tr>
<tr>
<td>Copying/Printing: Pages 1 through 25</td>
<td>$1.00 per page / electronic: $2.00 per page</td>
</tr>
<tr>
<td>Copying/Printing: All pages after first 25</td>
<td>$0.25 per page / electronic: $0.50 per page</td>
</tr>
<tr>
<td>Copying/Printing: Labor</td>
<td>$7.00 per hour</td>
</tr>
<tr>
<td>Electronic Media: Cost</td>
<td>CD or DVD: no charge; $5.00 per USB device</td>
</tr>
<tr>
<td>Postage</td>
<td>By weight</td>
</tr>
</tbody>
</table>

Back to Table of Contents
SECTION 3: USES AND DISCLOSURES OF PHI

3.7. Fundraising

A. POLICY

1. **Uses and Disclosures for Fundraising:** The University of Florida (UF) will use and disclose protected health information (PHI) for fundraising purposes only as permitted by the federal privacy regulations and relevant Florida laws.

2. **Approval Required:** Fundraising communications must be reviewed by the Privacy Office before they are sent out. Fundraising activities that do not meet the following Privacy Requirements must be approved in writing by the Privacy Office.

3. **Written authorization:** is required from patients for uses or disclosures of their PHI that exceed federal or state defined limits for fundraising. Without a more specific written authorization from the patient, UF may only use (internally) or disclose (to an external business associate) a limited amount of PHI, as defined by the Privacy Rule, for the purpose of raising funds for its own benefit.

4. **Opting-Out:** Patients are permitted to “opt out” of receiving solicitations and materials, whether verbal or written, concerning fundraising. UF shall:
   a. In a clear and conspicuous manner, provide an opportunity for the recipient of the communications to elect not to receive any further such communication;
   b. Provide methods for opting out that will not cause the recipient to incur an undue burden or more than a nominal cost.
   c. Make every effort to ensure that individuals who request to opt out of receiving fundraising communications do not receive them.

5. **Opt-Out Log:** The Privacy Office maintains a log of all individuals who request, in writing, not to receive any healthcare-related solicitations and materials concerning fundraising from UF, in part or in whole. Prior to use, all mailing lists and call lists prepared for healthcare-related fundraising must be forwarded to the Privacy Office for review and removal of any individuals who have opted out.

6. **Institutionally-related foundations involved in fundraising** for UF’s Health Science Center must:
   a. Sign a statement annually attesting to compliance with HIPAA regulations.
   b. Have written authorization from the patient or the patient’s legal representative to collect or maintain other data (beyond what is allowed by HIPAA) about individual patients.
   c. Have a valid Business Associate Agreement in place in addition to a contract for services before an external fundraiser may use the PHI. The business associate must agree to only use the PHI for UF’s fundraising activities.

B. DEFINITIONS

1. **Fundraising:** To solicit and acquire monetary and other resources for an institution or organization; an activity "for the specific purpose of raising funds" for the institution, rather than a general charitable purpose.
SECTION 3: USES AND DISCLOSURES OF PHI

3.7. Fundraising (continued)

2. **Institutionally-related Foundation**: One qualified under the tax code (e.g., 501(c)3) that has an "explicit linkage" to the covered entity, or to a group of organizations of which the covered entity is one. "The term does not include an organization with a general charitable purpose, such as to support research about or to provide treatment for certain diseases" even if some of its resources may be given to the covered entity.

**C. PRIVACY REQUIREMENTS**

1. **PHI for Fundraising**: A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following PHI, for the purpose of raising funds for its own benefit, without an authorization:
   
   a. Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;
   
   b. Dates of health care provided to an individual.
   
   c. Department of service information;
   
   d. Treating physician;
   
   e. Outcome information; and
   
   f. Health insurance status, (i.e., whether the patient has health insurance or not: the insurance carrier’s name, type of insurance, amounts of coverage, etc., as well other payment arrangements, are not included.)

   NOTE: Information specifically concerning the patient’s diagnoses is not included.

2. **Fundraising Requirements**: The covered entity may not use or disclose PHI for fundraising purposes as otherwise permitted by the Privacy Rule unless a statement concerning the use and disclosure is included in the covered entity’s notice [of privacy practices].

   a. With each fundraising communication made to an individual, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications.

   b. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

   c. A covered entity may not condition treatment or payment on the individual’s choice with respect to the receipt of fundraising communications.

   d. A covered entity may not make fundraising communications to an individual where the individual has elected not to receive such communications.

   e. A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.
SECTION 3: USES AND DISCLOSURES OF PHI

3.7. Fundraising (continued)

D. PROCEDURES

1. **Clearly and conspicuously include Opt-Out instructions** in all fundraising materials or solicitations, when calling or sending out to patients. These instructions should include:
   a. A written or verbal description of how the recipient may “opt out” of receiving further such communications (i.e., to affirm their wish to be excluded from further communications).
   b. A description of how the patient, by completing and signing a “request for more information” form or a more specific authorization, may give permission for UF to use or disclose the patient’s specified PHI for a fundraising purpose.

2. **Obtain written authorizations** from patients prior to using or disclosing any information about them if the information will be used in or for fundraising materials or publications, including, but not limited to, patient photographs and testimonials.

3. **Requests to Opt-Out**: Immediately report to the Privacy Office any communications from patients and others who have requested to opt out of receiving future fundraising communications to ensure that no more communications are sent.

4. **Forward all letters, communication scripts, and mailing and call lists** prepared for healthcare-related fundraising purposes to the Privacy Office for review prior to sending out any materials or making calls.
   a. Mailing and call lists should be in spreadsheet format, and include only names and addresses of recipients. Telephone numbers may also be included to improve identification.
   b. Scripts for calls must be in writing and approved by the Privacy Office prior to use.

5. **Upon request, provide an Authorization to Use or Disclose Protected Health Information** form (see Forms) and/or a “request more information” form specifically developed for fundraising and approved by the Privacy Office. Use the **Authorization to Use or Disclose PHI for Marketing, Fundraising, Publications or Public Relations** form. (See Forms)

6. **Maintain signed request or authorization forms** from those persons who have specifically agreed to receive more specific fundraising communications, based on their written authorization for at least six years. (See SECTION 3: Uses and Disclosures of PHI: Authorizations.)

E. REFERENCES

**HIPAA**: 45 CFR §164.501 Definitions, §164.514(f) Fundraising Communications

F. EXHIBITS

[Attestation of Compliance for Fundraising]

[Back to Table of Contents]
SECTION 3: USES AND DISCLOSURES OF PHI

3.8. Marketing

A. POLICY

1. Uses and Disclosures for Marketing: The University of Florida (UF) will use and disclose protected health information (PHI) for marketing purposes only as permitted by the federal privacy regulations and relevant Florida laws.

2. Approval Required: Marketing communications must be reviewed by the UF Privacy Office before they are sent out. Marketing activities that do not meet the Privacy Requirements below must be approved in writing by the Privacy Office.

3. Written authorization: is required from patients for all treatment and health care operations communications where UF or its business associates receive financial remuneration for making the communications from a third party whose product or service is being marketed, and for any other uses or disclosures of PHI which specifically qualify as marketing. The authorization must indicate that UF and/or the business associate will receive either direct or indirect remuneration for the provision of the PHI. The following activities are not subject to HIPAA regulations:
   a. Marketing activities that do not use PHI to target a specific group of individuals, including mass mailings and communications such as newsletters that do not use PHI to identify the recipients of the mailing;
   b. Communications promoting health in general and that do not promote a product or service from a particular provider, such as communications promoting a healthy diet or encouraging individuals to get certain routine diagnostic tests;
   c. Communications about government and government-sponsored programs, as there is no commercial component to communications about benefits through public programs.

4. Opt-Out Log: The Privacy Office maintains a log of all individuals who request not to receive any healthcare-related solicitations and materials concerning fundraising and/or marketing from UF, in part or in whole. All mailing lists prepared for healthcare-related marketing must be forwarded to the Privacy Office prior to mailing for review and removal of any individuals who have opted out.

5. Sale of PHI Prohibited: UF and its business associates may not sell PHI, including, but not limited to, lists of patients or enrollees, to any third party for that party’s marketing use without obtaining authorization from each patient or the patient’s legal representative. The authorization must indicate whether UF and/or the business associate will receive direct or indirect remuneration for the provision of the PHI.

B. DEFINITIONS

1. Face to face communications: conversations in which two or more people are physically located in the same room; does not include any communications made over the phone, sent through the mail or via e-mail.
SECTION 3: USES AND DISCLOSURES OF PHI

3.8. Marketing (continued)

2. **Financial remuneration:** Direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual. “Financial remuneration” does not include non-financial benefits, such as in-kind benefits, provided to a covered entity in exchange for making a communication about a product or service.

3. **Marketing:** To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

Marketing does **not** include a communication made:

1) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity’s cost of making the communication.

2) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:
   a) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;
   b) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or
   c) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

4. **Subsidized Treatment Communications:** Communications specifically related to the treatment of a patient where the covered entity receives financial remuneration for making the communications from a third party whose product or service is being marketed.

C. PRIVACY REQUIREMENTS

1. **Marketing – Florida Statutes:** “Absent a specific written release or authorization permitting utilization of patient information for solicitation or marketing the sale of goods or services, any use of that information for those purposes is prohibited.” (F.S. 456.057(7)(b))

2. **Marketing – HIPAA:**
   a. A covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:
SECTION 3: USES AND DISCLOSURES OF PHI

3.8. Marketing (continued)

1) A face-to-face communication made by a covered entity to an individual; or
2) A promotional gift of nominal value provided by the covered entity.

b. If the marketing involves financial remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved. The financial remuneration a covered entity receives from a third party must be for the purpose of making a communication and such communication must encourage individuals to purchase or use the third party’s product or service.

c. Where a business associate (including a subcontractor), as opposed to the covered entity itself, receives financial remuneration from a third party in exchange for making a communication about a product or service, such communication also requires prior authorization from the individual.

D. PROCEDURES

1. Use the Authorization to Use or Disclose PHI for Public Activities form (see Forms) to obtain written authorizations from patients prior to:

   a. Providing subsidized treatment communications to patients, if the communication will not be made face-to-face by someone from UF or does not consist of a promotional gift of nominal value provided by UF;

   b. Using or disclosing any information about or from the patient if the information will be used in or for marketing purposes, including, but not limited to, patient photographs and testimonials.

2. Immediately report to the Privacy Office any communications from patients and others who have requested to stop receiving future marketing communications to ensure that no more communications are sent.

3. Forward all letters, communication scripts, and mailing and call lists prepared for healthcare-related marketing purposes to the Privacy Office for review prior to sending out any materials. Mailing lists should be in spreadsheet format, and only need to include names and addresses of recipients.

4. Provide Authorization to Use or Disclose PHI forms (see Forms) as necessary for marketing activities. Maintain signed authorization forms from those persons who have specifically agreed to receive more specific marketing communications, based on their written authorization for at least six years. (See SECTION 3: Uses and Disclosures of PHI: Authorizations.)

E. REFERENCES:

1. HIPAA: 45 CFR §164.501 Definitions, §164.508(a)(3) Authorization required: Marketing,
2. Florida Statutes: 456.057(7)(b) Ownership and control of patient records: Marketing

F. EXHIBITS:

None

Back to Table of Contents
SECTION 3: USES AND DISCLOSURES OF PHI

3.9. Research

A. POLICY

1. Uses and Disclosures for Research: The University of Florida (UF) will use and disclose protected health information (PHI) for research involving human subjects in accordance with the federal privacy, security, and research regulations.

2. Authorization: PHI may not be used or disclosed for research without the individual authorization of the patient or written approval (waiver of authorization) from UF’s Institutional Review Board (IRB). “Perusing”, “trolling”, “chatting about”, or otherwise informally gathering PHI about individuals with whom the researcher does not have a formal provider/patient relationship is prohibited.

3. De-identified Health Information: Health information that has been de-identified is no longer protected and may be used for research without patient authorization. Prior written informed consent/authorization of patients for the research use of their health information, currently existing in a de-identified state, is not required.

4. Honest Broker Services: PHI can either be de-identified by an honest broker that is part of a UF-designated health care component or by an honest broker that is a business associate of the covered entity. The honest broker cannot be one of the investigators or associated with the research team for which the honest broker performs duties.

B. DEFINITIONS

1. Certification of Review: Approvals available from the IRB for a researcher to access PHI either in preparation for conducting research, or for conducting research using decedent information.

2. Compound Authorizations: An authorization for use or disclosure of protected health information that has been combined with another document for a research study.

3. De-Identification: Rendering PHI so that it is not individually identifiable. (See Appendix A: Glossary for the full definition.)

4. Honest Broker: an individual, organization or team acting for, or on behalf of, the covered entity to collect health information, de-identify it, and provide it to research investigators in such a manner that it would not be reasonably possible for the investigators or others to identify the corresponding patients-subjects directly or indirectly. At UF, all Honest Brokers must be certified through the Privacy Office. (See SECTION 6: Honest Broker Certification.)

5. Institutional Review Board: A committee established by UF to protect the rights and welfare of human subjects recruited to participate in research activities conducted under the auspices of UF. The IRB performs the functions of the privacy board for UF.
SECTION 3: USES AND DISCLOSURES OF PHI

3.9. Research (continued)

6. **Limited Data Set:** A data set which excludes all previously listed direct identifiers of the individual, or of relatives, employers, or household members, except for Town or city, State, and zip code; and Dates. (See Limited Data Sets and Data Use Agreements in the HIPAA Privacy Management manual.)

7. **Research:** Systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

8. **Waiver of Authorization:** Approval by the IRB for a researcher to use and disclose PHI for a research activity, including but not limited to, identifying, recruiting, and/or enrolling subjects without the patient’s permission.

**C. PRIVACY REQUIREMENTS**

1. **Use and Disclosure:** A covered entity may use or disclose PHI for research, regardless of the source of funding of the research, provided that the covered entity:
   a. De-identifies the health information, or
   b. Obtains authorization for the use or disclosure, including either:
      1) Individual authorization from the patients whose PHI will be used or disclosed during the research; or
      2) Documentation that an Institutional Review Board (IRB) has approved a Waiver of the required individual authorizations.

2. **Certification of Review Preparatory to Research** is available for researchers who are considering research studies and need to ensure that data is available or to identify potential subjects in order to obtain their authorization to use or disclose their PHI for a research study.
   a. Certifications will only be considered if the researcher indicates that:
      1) Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;
      2) No PHI will be removed from the covered entity by the researcher during the review; and
      3) The PHI for which use or access is sought is necessary for the research purposes.
   b. Identifiable information may be collected under this Certification of Review as necessary to prepare a research protocol or to aid in study recruitment, as long as the PHI is not removed from the covered entity.

Specifically, even though UF and Shands share a common electronic medical record system, PHI retrieved from records created as a result of encounters within UF facilities may be used by UF employees for purposes preparatory to research without a patient authorization or a waiver of authorization, but PHI retrieved from records created by an encounter within Shands entities would require either the patient’s authorization or an IRB waiver of authorization for the PHI to be used by UF employees.
SECTION 3: USES AND DISCLOSURES OF PHI

3. Certification for Decedent Research is available if a research study requires the use or disclosure of PHI of deceased individuals’. The researcher must show:
   a. That the use or disclosure sought is solely for research on the PHI of decedents;
   b. Documentation, if requested, of the death of such individuals; and
   c. That the PHI for which use or disclosure is sought is necessary for the research purposes.

4. Compound Authorizations: An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study.
   a. This includes combining an authorization for:
      1) The use or disclosure of protected health information for a research study,
      2) With another authorization for the same research study, or
      3) With an authorization for the creation or maintenance of a research database or repository, or
      4) With a consent to participate in research.
   b. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

5. Accounting of Disclosures: Certain disclosures of PHI being used under a Waiver of Authorization or a Certification must be tracked for Accounting of Disclosures purposes. (See SECTION 4: Patient Rights: Accounting for Disclosures in this manual.)

D. PROCEDURES

1. Using an Honest Broker: For an individual, organization or team to be an Honest Broker for UF, the proposed honest broker must be certified pursuant to the process described in the Policy for Honest Broker Systems, found in the HIPAA Privacy Management Manual.

2. Requesting Health Records, Health Information, or Health Data:
   a. Prior to requesting or reviewing PHI, obtain authorization from the study subjects, or if obtaining such authorizations is impracticable or impossible, apply for an IRB Certification for Review or a Waiver of Authorization.
   b. For retrospective chart reviews where the identity of potential subjects is not known, use a Waiver or a Certification to direct requests for patient health information to the Decision Support Services of either UF or Shands; data reports may be used to more specifically identify potential subjects or to narrow the range of records that will need to be reviewed to identify potential subjects.
      1) Do not ask clinic or department managers to produce lists of identifiable patient information from their data access resources.
SECTION 3: USES AND DISCLOSURES OF PHI

3.9. Research (continued)

2) Provide copies of IRB documentation, showing exactly what was approved for use, to the UF or Shands Privacy Office, depending on which institution holds the patient information.

3. Using Compound Authorizations: Clearly define the conditioned and unconditioned parts of the research protocol, and provide appropriate methods for subjects to clearly “opt in” (sign up for) each component of the authorization. Suggested methods include:
   a. Use a separate check-box requiring the patient’s initials for the unconditioned research activity to signify whether an individual has opted-in, while maintaining one signature line for the authorization, or
   b. Provide a distinct signature line for authorization of the unconditioned research activity to signal that the individual is authorizing optional research that will not affect research-related treatment.

4. Retention and Storage of Documents:
   a. Any paper documents or electronic media used in research that contain PHI or other restricted data must be stored in accordance with UF’s information security standards. (See SECTION 2: Health Information Management: Retention, Archiving, and Storage in this manual)
   b. Any documentation specifically required by HIPAA regulations must be retained for a minimum of six years (Authorizations, Waivers, Certificates, etc.).
   c. Research documents containing PHI may be digitally created or imaged from paper and stored electronically, provided that all UF security requirements are met.
      1) Electronic research records containing PHI must be stored securely and backed up sufficiently to prevent loss of documentation in the event of electronic malfunctions or other events.
      2) No unencrypted PHI may be stored on a portable data management device or on the hard-drive of a desktop or laptop computer.

5. Research on Three or Fewer Subjects is generally considered case-reporting rather than research. However, this activity often still requires IRB involvement. See the IRB-01 website Help-link: “Do I need approval for a Case Report?” at http://irb.ufl.edu/irb01/help/case.html for more information.
   a. If IRB involvement is not required, the use of identifiable patient information must be authorized in writing by the patients or their legal representatives. Authorizations should clearly define what information will be used, what it will be used for, and who is expected to have access to it.
   b. If the information to be used has been de-identified, no authorizations are needed from the patients; however, use of the information must be approved by the Privacy Office.

6. Correcting Improper Procedures:
   a. Failure to Obtain Authorization: In the event that a Principle Investigator (PI) fails to obtain proper authorization from individual subjects before beginning research or reviews preparatory to research, the PI will either re-consent the subjects or destroy the data and specimens already collected. The PI must attest to, in writing, which option was chosen and its completion date in a letter to the Chief Privacy Officer.
SECTION 3: USES AND DISCLOSURES OF PHI

3.9. Research (continued)

1) Re-consenting: Obtain the IRB-approved authorization from individual subjects within 30 calendar days of identification of the faulty authorization.
   a) The letter must be received in the Privacy Office within 5 business days after the 30-day cut-off date.
   b) Authorizations may be obtained by mail from individual subjects. Letters requesting such authorization must be post-marked within the 30-day re-consenting period.

2) Destroying Data and Specimens: Immediately destroy all data and corresponding specimens collected under the faulty authorization. The letter must be received in the Privacy Office within 5 business days after the failure to obtain a proper authorization is identified and reported.
   b. Failure to Obtain Waiver of Authorization: In the event that a PI fails to obtain a proper Certification or Waiver of Authorization from the IRB before beginning research or reviews preparatory to research,
      1) The PI will immediately destroy all data and corresponding specimens affected.
      2) The PI must attest in writing that the data and specimens were destroyed and the completion date in a letter to the Chief Privacy Officer. The letter must be received in the Privacy Office within 5 business days after the failure to obtain a proper waiver is identified and reported.

E. REFERENCES

1. HIPAA: 45 CFR §164.508(b) Authorizations; §164.512(i) Uses and disclosures for research purposes

F. EXHIBITS:

None

Back to Table of Contents
SECTION 3: USES AND DISCLOSURES OF PHI

3.10. Sale of Protected Health Information

A. POLICY

NEW: 09/01/2013

1. Sale of Protected Health Information: The University of Florida (UF) will not sell protected health information (PHI) for any purpose except as allowed and in accordance with the federal privacy and security regulations.

2. Authorization required: UF must obtain an authorization from each affected patient for any disclosure of their PHI which meets the definition of a sale of PHI, as defined in the Privacy Rule; the authorization must state that the disclosure will result in remuneration to UF.

B. DEFINITIONS

1. Protected Health Information (PHI), as defined by HIPAA:
   a. Individually identifiable health information transmitted by or maintained in electronic media, or in any other form or medium.
   b. PHI excludes individually identifiable health information found:
      1) in Education records covered by the Family Education Rights and Privacy Act (FERPA);
      2) in Employment records held by a covered entity in its role as an employer.
      3) Regarding a person who has been deceased for more than 50 years.

2. Sale of PHI: For purposes of this policy, a disclosure of PHI by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the PHI.

C. PRIVACY REQUIREMENTS

   a. A covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined by HIPAA.
   b. Such authorization must state that the disclosure will result in remuneration to the covered entity.

2. Sale of PHI does not include:
   a. A disclosure of PHI for public health purposes described at § 164.512(b);
   b. A disclosure of PHI for research purposes, where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;
   c. A disclosure of PHI for treatment and payment purposes;
   d. A disclosure of PHI for the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in the definition of health care operations;
SECTION 3: USES AND DISCLOSURES OF PHI

3.10. Sale of Protected Health Information (continued)

   e. A disclosure of PHI to or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, for the performance of such activities;

   f. A disclosure of PHI to an individual, when requested under an individual’s right to access personal records or when requesting an accounting of disclosures;

   g. A disclosure required by law as permitted under the Privacy Rule; and

   h. A disclosure for any other purpose permitted by and in accordance with the applicable requirements of the Privacy Rule, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

D. PROCEDURES

   For assistance in determining if a transaction involving the transfer of health information meets the definition of a sale of PHI, call the Privacy Office.

E. REFERENCES

   HIPAA: 45 CFR §164.508(a)(4) Authorization required: Sale of protected health information;

F. EXHIBITS

   Authorization for the Sale of Protected Health Information
SECTION 4: PATIENT’S RIGHTS

4.1. The Notice of Privacy Practices

A. POLICY

1. Notice: Patients or their personal representatives will be notified of their privacy rights and of how the University of Florida (UF) may use their protected health information (PHI) before they enter the health care system at any point, including home visits, in accordance with current federal and state laws.

2. Availability: Paper copies of the Notice are provided to every new patient and are available at any time upon request. The Notice is also posted in conspicuous locations in UF’s patient care areas, as well as on UF’s Privacy Office web site.

3. Changes in the Notice: If UF’s privacy practices change, patients will be notified of the change by making the updated notice accessible as noted above and available at service delivery sites for individuals to request on or after the effective date of the revision.

4. OHCA: UF participates in an Organized Health Care Arrangement (OHCA) with the Shands HealthCare System; any member of the OHCA may provide a Notice of Privacy Practices to a patient at the first delivery of service.

B. DEFINITIONS

1. Notice of Privacy Practices: A statement, mandated by federal and state laws, which outlines how UF and its affiliates will use and disclose patients’ protected health information (PHI) and how patients may gain access to that information.

2. Acknowledgement of Receipt: A statement, mandated by federal law and preferably signed by the patient, indicating that the patient received the Notice of Privacy Practices.

C. PRIVACY REQUIREMENTS

1. Notice: An individual has a right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity, and of the individual’s rights and the covered entity’s legal duties with respect to PHI.

2. Required Notice Elements: The covered entity must provide a notice that is written in plain language and that contains the following required elements:
   a. Header: The notice must contain the following statement as a header or otherwise prominently displayed: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”
   b. A description, including examples, of the types of uses and disclosures that the covered entity is permitted to make for the purposes of treatment, payment, and health care operations. A description of each of the other purposes for which the covered entity is permitted or required to use or disclose PHI without the individual’s written authorization. Each of these description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by the Privacy Rule and other applicable law.
SECTION 4: PATIENT’S RIGHTS

4.1. The Notice of Privacy Practices (continued)

   c. A statement indicating that most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require authorization.

   d. A statement regarding fundraising communications and an individual’s right to opt out of receiving such communications.

   e. A statement that other uses and disclosures not described in the NPP will be made only with the individual’s written authorization and that the individual may revoke such authorization.

   f. A statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

   g. A statement that the covered entity is required by law to maintain the privacy of PHI, to provide individuals with notice of its legal duties and privacy practices with respect to PHI, and to notify affected individuals following a breach of unsecured PHI; that the covered entity is required to abide by the terms of the notice currently in effect; and that the covered entity reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains. The statement must also describe how it will provide individuals with a revised notice.

   h. The notice must contain the name, or title, and telephone number of a person or office to contact for further information, and the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

3. Health care providers are required to include a statement informing individuals of their right to restrict certain disclosures of protected health information to a health plan where the individual pays out of pocket in full for the health care item or service.

4. Revisions to the Notice: The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual’s rights, the covered entity’s legal duties, or other privacy practices stated in the notice.

5. Providing the Notice: A covered health care provider that has a direct treatment relationship with an individual must:
   a. Provide the notice no later than the date of the first service delivery, including service delivered electronically, to such individual; or as soon as reasonably practicable after an emergency treatment situation;
   b. Make a good faith effort to obtain a written acknowledgment of receipt of the notice provided;
   c. Have the notice available at the service delivery site for individuals to request to take with them;
   d. Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice;
SECTION 4: PATIENT’S RIGHTS

4.1. The Notice of Privacy Practices (continued)

e. Whenever the notice is revised, make the notice available upon request on or after the effective
date of the revision.

f. A covered entity that maintains a web site that provides information about the covered entity’s
customer services or benefits must prominently post its notice on the web site and make the notice
available electronically through the web site.

D. PROCEDURES

1. Give the Notice of Privacy Practices (see Forms) to every patient or personal representative before or
at the first delivery of service. Provide a new copy of the NPP whenever the notice has been updated,
even if the patient has received a notice before.

2. Ask the patient to sign the Acknowledgement form when they receive the notice. (See Forms)
   a. If a patient cannot or will not sign the acknowledgement, note the reason on the form and any
efforts made to obtain the signature.
   b. The patient may be treated whether the acknowledgement is signed or not.

3. Give the patient a copy of the acknowledgement form, whether the patient signed it or not. File the
original acknowledgement form in the patient’s health record.

4. Enter any appropriate tracking information in the computer-based or other tracking system
designated for this purpose, to indicate that the patient received the NPP.
   a. When a patient returns to UF or Shands, at any point of entry, determine whether the patient has
      received the most current version of the NPP by checking the tracking system.
   b. Follow the procedure above to give a new patient the most current NPP, or, if the NPP has been
      updated, to give a returning patient the most current version.
   c. No action is required if the system indicates the patient has already received a current NPP.
      However, if in doubt, provide another NPP and have the patient sign an acknowledgment.

E. REFERENCES

HIPAA: 45 CFR §164.501 (Definitions); § 164.520 (Notice of Privacy Practices)

F. EXHIBITS

1. Notice of Privacy Practices: English and Spanish (Forms)
2. Acknowledgement of Receipt: English and Spanish (Forms)

Back to Table of Contents
SECTION 4: PATIENT’S RIGHTS

4.2. Access to Personal Health Records

A. POLICY

1. **Right to Inspect or Receive Copies:** In general, patients and/or personal representatives have the right to inspect and/or receive copies of personal health information that is maintained in a designated record set by the University of Florida (UF). However, when a patient’s psychiatric, psychological, or psychotherapeutic records are requested by the patient or representative, the patient’s healthcare provider may elect to provide a report of examination and treatment in lieu of copies of records.

2. **The Right of Access Does Not Apply to:**
   a. PHI that is subject to the Clinical Laboratories Improvements Amendment of 1988 (currently under review and subject to change);
   b. Psychotherapy notes;
   c. Information being compiled for a legal proceeding.

3. **Authorizations:**
   a. For Treatment Purposes: A signed authorization is not required to provide copies of patient records to another healthcare provider for treatment purposes; however, an authorization may be requested at the discretion of the clinic or department manager.
   b. For Non-Treatment Purposes: Requests for access to personal health records for purposes not related to treatment, must be made in writing by the patient or the patient’s legal representative, using the forms provided on the UF Privacy website.
   c. Authorization Delivery: Record request forms and authorizations may be delivered in person, or by mail or fax; signed forms may also be scanned and e-mailed to the appropriate record owner/custodian.

4. **Deceased Patients:** Access to records of a deceased patient must be authorized in writing by:
   a. The Executor/trix of the patient’s estate,
   b. The surviving spouse,
   c. A documented healthcare decision-maker appointed by the patient,
   d. The legal next-of-kin.

5. **UF will respond** to all requests for access within 30 days of receiving the written request. If the request cannot be fulfilled within 30 days, UF will notify the requestor of the delay and will fulfill the request within 60 days, as allowed by the Privacy Rule.

6. **UF will charge a reasonable fee** for producing copies of health records and for appointments to view records when the copies or the viewing are for purposes not related to treatment. (See Copying and Inspection Fees table at the end of this chapter.)

7. **Format:** Generally, record copies will be produced in hard-copy or paper format. UF will make reasonable efforts to accommodate requests for record copies in electronic formats.
SECTION 4: PATIENT'S RIGHTS

4.2. Access to Personal Health Records (continued)

B. DEFINITIONS

1. **Clinical Laboratories Improvements Amendment of 1988**: established quality standards for all laboratory testing to ensure the accuracy, reliability and timeliness of patient test results regardless of where the test was performed. However, the law generally only allows patients to receive test results through their physicians. (§ 493.1291(f))

2. **Designated Record Set**: A defined group of health and billing records that contain PHI maintained by UF and used to help make decisions about patients. (See the full definition in Appendix A: Glossary; see also SECTION 2: Health Information Management: Designated Record Set in this manual.)

3. **Inspect**: To visually review the original record elements that are part of the designated record set whether maintained in paper or electronic formats.

4. **Receive a Copy**: To obtain a photocopy or print-out of record elements that are part of the designated record set whether maintained in paper or electronic formats.

C. PRIVACY REQUIREMENTS

1. **Patients and legal representatives may view** the patient’s designated record set in the presence of an authorized UF staff member.

2. **Patients and legal representatives may have copies** of the patient’s designated record set, subject to a reasonable copying fee that includes labor and postage, if appropriate. The patient must be notified of the fee amount prior to copies being made.

D. PROCEDURES

1. **Authorization and Verification**:
   a. When necessary, ask the patient or representative to complete an Authorization to Use or Disclose Protected Health Information (see policies above; also see Forms; also see SECTION 3: Uses and Disclosures of PHI: Authorizations in this manual).
   
   b. Make reasonable efforts to verify the identity of the person making the request, and if not the patient, their relationship to the patient and authority to access the patient’s PHI. (See SECTION 1: Verification of Identity and Authority in this manual.) If a patient or legal representative has documents to corroborate identity or authority, make and attach copies to the authorization form.
   
   c. If the records requested are psychiatric, psychological, or psychotherapeutic, notify the patient’s healthcare provider for further instructions; the provider may elect to provide a summary report of examination and treatment instead of actual copies of records.
SECTION 4: PATIENT’S RIGHTS

4.2. Access to Personal Health Records (continued)

2. To Receive Copies of Records:
   - For purposes not related to treatment:
     a. After receiving the completed authorization form, inform the patient or representative of the copying charges that will apply. (See Copying and Inspection Fees chart at the end of this chapter.)
     b. Forward the completed Authorization form to the person designated to produce copies of records for your area.
   - For treatment-related purposes:
     a. Ask the patient or representative for the name and address, fax number, or e-mail address of the care giver to whom the copies should be sent; or
     b. If the request is urgent (i.e. an appointment the next day), make other reasonable arrangements with the patient for supplying the needed information to the new care provider.
        a) Giving the copies directly to the patient for transport,
        b) Scanning and e-mailing the pertinent information in an encrypted or other protected format, or
        c) Faxing the information.
     3) There is no charge for providing copies of records for treatment purposes.
   - Producing copies: Provide copies of requested records in the format specified by the patient or representative, if possible.
     a. Paper copies should be printed or photocopied from original materials.
     b. Electronic copies may be produced on a CD, DVD, USB drive or other appropriate recording media. Do not use electronic storage media provided by a patient.
     c. Electronic storage media must be encrypted. Provide the encryption key to the patient by a separate means (letter, (authorized) e-mail, or hand-delivery).

   NOTE: Physicians, at their discretion, may authorize the release of a copy of a lab or other report to the patient or representative at the time of providing care, without requiring a written authorization.

3. To Inspect or View Personal Health Records:
   a. After receiving a completed and verified Authorization form, schedule an appointment for the patient and/or representative to visually inspect records at the earliest opportunity, but no more than 30 days from the date of the request.

   NOTE: Patients and personal representatives may only review records in the company of a UF or Shands representative.
   b. Record the appointment date and time on the Authorization form and forward the form to the clinic or department manager.
     1) If the inspection is for purposes not related to treatment: The manager notifies the patient’s health care provider of the appointment date and time. Together they decide who will sit with the patient during the inspection.
SECTION 4: PATIENT’S RIGHTS

4.2. Access to Personal Health Records (continued)

2) If the inspection is for treatment-related purposes: Ensure that the care giver knows the patient has requested to view the health record during the appointment.

c. Prior to the appointment, prepare the paper record for inspection by removing all parts of the health record that are not included in the designated record set (see SECTION 2: Health Information Management: Designated Record Set). For electronic records, make a list prior to the appointment of all components to be viewed.

NOTE: Patients or their representatives may not personally alter any part of a health record during the inspection, but may make notes and request an amendment or correction, using the Request for Amendment of a Health Record form and procedure.

d. After the inspection, document on the Authorization form the participants and the date and time that the inspection took place. File or scan the original form into the patient’s health record (paper or electronic). Give the original or a copy of the annotated authorization form to the patient or representative who inspected the records, depending on whether the form will go into a paper or electronic record. If paper, keep the original and give the patient a copy; if electronic, scan the original and then give it to the patient.

E. REFERENCES

1. HIPAA: 45 CFR §164.501 Definitions; §164.524 Right of Access

2. Florida Statutes: 456.057 Ownership and control of patient records; report or copies of records to be furnished.

F. EXHIBITS

Copying, Production, and Inspection Fees

Authorization to Use and Disclose PHI (Forms)

Back to Table of Contents

<table>
<thead>
<tr>
<th>Services</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspection of Records: Per hour</td>
<td>$25.00</td>
</tr>
<tr>
<td>Copying/Printing: Pages 1 through 25</td>
<td>$1.00 per page / electronic: $2.00 per page</td>
</tr>
<tr>
<td>Copying/Printing: All pages after first 25</td>
<td>$0.25 per page / electronic: $0.50 per page</td>
</tr>
<tr>
<td>Copying/Printing: Labor</td>
<td>$7.00 per hour</td>
</tr>
<tr>
<td>Electronic Media: Cost</td>
<td>CD or DVD: no charge; $5.00 per USB device</td>
</tr>
<tr>
<td>Postage</td>
<td>By weight</td>
</tr>
</tbody>
</table>
SECTION 4: PATIENT’S RIGHTS

4.3. Request to Restrict Uses and Disclosures of PHI

A. POLICY

1. The University of Florida (UF) permits patients and personal representatives to request restrictions of uses and disclosures of protected health information (PHI) for treatment, payment, or health care operations. Such requests must generally be made in writing.

2. Written requests for restrictions of uses and disclosures of PHI will be reviewed individually and every effort made to accommodate reasonable requests. Completed request forms may be delivered in person, or by mail or fax; signed forms may also be scanned and e-mailed.

3. Certain Requests for Restrictions Required: UF must comply with a patient/representative’s request to restrict certain PHI if the disclosure is to a health plan for payment purposes and, the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

4. Decisions to grant or deny a request for restriction of PHI, other than those specifically mandated by law, are coordinated and approved through the UF Privacy Office. No decision will be made unilaterally by a clinic or department manager or by the Privacy Office. Only clinic or department managers, with the approval of the Privacy Officer, may grant or deny restrictions. Any restriction agreed to by any other person will not be valid.

5. Changes or Additions: Requests for changes in currently granted restrictions or for new restrictions in addition to ones already granted must be resubmitted on a new Request for Special Privacy Protections form. The new form should include all restrictions requested, not just the most recent request, and will supersede all previous request forms of the same type.

6. Follow Up: The designated management representative must ensure that all records to which the restriction applies, including both health and financial records, are appropriately flagged.

7. Termination of Restrictions: UF may terminate its agreement to a restriction, if:
   a. The patient or representative agrees to or requests the termination in writing; or
   b. UF informs the patient or representative that it is terminating its agreement to a restriction. Such terminations are only effective with respect to PHI created or received after the patient has been informed.

B. DEFINITIONS

Restriction: A specifically defined limitation of use or disclosure of an element of PHI that would normally be available for use or disclosure by a health care provider in the normal course of business for treatment, payment or health care operations.
SECTION 4: PATIENT’S RIGHTS

4.3. Request to Restrict Uses and Disclosures of PHI (continued)

C. PRIVACY REQUIREMENTS

1. Right to Request Restrictions: A covered entity must permit an individual to request that the covered entity restrict uses or disclosures of PHI about the individual to carry out treatment, payment, or health care operations, or related to disclosures that are allowed unless the patient objects, i.e., disclosures related to a facility directory and disclosures to family or friends involved in the patient’s care.

2. Right to Deny Requests: A covered entity is not required to agree to a restriction of PHI, unless the following conditions apply:
   a. The disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and
   b. The PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

3. Limitations: A covered entity that agrees to a restriction may not use or disclose PHI in violation of such restriction, except in cases where the patient is in need of emergency treatment and the information is essential to the treatment.

4. Terminating a Restriction: A covered entity may terminate its agreement to a restriction, if:
   a. The individual agrees to or requests the termination in writing;
   b. The individual orally agrees to the termination and the oral agreement is documented; or
   c. The covered entity informs the individual of the termination; such termination is only effective for PHI created or received after the individual has been informed.

D. PROCEDURE

1. Verify Identity and Authority: Make reasonable efforts to verify the identity of the person requesting the restriction, and if not the patient, their relationship to the patient and authority to make the request. (See SECTION 1: Verification of Identity and Authority in this manual.) If a patient or legal representative has documents to corroborate identity or authority, attach copies to the Request form.

2. Provide Assistance: Assist the patient or representative to complete a Request for Special Privacy Protections form (see Forms). Give the requestor a copy of the completed form.

3. Restrictions Requested for Out-of-Pocket Payments: If a health care provider will be paid out of pocket in full by the patient, and the patient requests that no PHI be disclosed to the patient’s health plan for payment purposes, the provider’s department or unit must follow its process established for such a restriction. Completion of a Request for Special Privacy Protections form is not required.

4. Response Coordination: If a request for a restriction of PHI requires assistance from the Privacy Office, forward the completed Request form to the appropriate Privacy Office as soon as possible. Responses to these requests are the responsibility of the Privacy Office.
SECTION 4: PATIENT’S RIGHTS

4.3. Request to Restrict Uses and Disclosures of PHI (continued)

   a. If the request is denied, the denial of restriction and the reason(s) will be documented by the Privacy Office on the Response to Request for Special Privacy Protections form or in a letter. Place copies of the request and the response in the patient’s health record. (The original documents will be filed in the Privacy Office.)

   b. If the request is granted, the response will be documented by the Privacy Office on the original request form. Place a copy of the completed Request for Special Privacy Protections in the patient’s health record. (The original document will be filed in the Privacy Office.)

      1) Place an alert/notification in the patient’s chart to alert all staff to the restriction.
      2) Notify all staff affected by the restriction to ensure its implementation in operational activities.
      3) Notify your supervisor and/or the Privacy Office immediately if there are any difficulties in abiding by the restriction, or of any problems that occur as a result of the restriction.

   c. If the restriction is terminated or changed, the Privacy Office will provide a copy of the Termination of Special Privacy Protection form to both the patient and the clinic or department:

      1) File the Termination form in the patient’s health record, and make appropriate changes in the record or other documentation to indicate that the restriction has been terminated.
      2) Notify all staff affected by the termination of restriction to ensure that the change is implemented in operational activities.

   5. Retain all documentation for at least six years after the date that it was last in effect.

E. REFERENCES

   HIPAA: 45 CFR §164.501 - Definitions; §164.522 - Right to Request Privacy Protections

F. EXHIBITS

   Form: Request for Special Privacy Protections

Back to Table of Contents
SECTION 4: PATIENT’S RIGHTS

4.4. Request for More Confidential Communications

A. POLICY

1. **The University of Florida (UF) permits** patients and personal representatives to request to receive communications of protected health information (PHI) from their provider by alternative means or at alternative locations. Such requests must generally be made in writing.

2. **Written requests for more confidential communications** of health information will be reviewed individually and every effort made to accommodate reasonable requests. Completed request forms may be delivered in person, or by mail or fax; signed forms may also be scanned and e-mailed.

3. **Verbal/Aural Communications:** Patients may request an alternative location or method for face-to-face or telephone discussions or provision of health information at any time. Staff members should make reasonable accommodations for such requests at the time they are received.

4. **Written Communications:** Patients may request to receive written communications (reports, bills, etc.), which require more than a change of address or other demographics, in an alternative manner or location.
   a. Any requests of this type that are referred to the Privacy Office should be extraordinary requests requiring special arrangements outside the normal course of business operations.
   b. The decision to grant or deny a request will be based on:
      1) The ability or inability of UF to consistently accommodate such a request, and
      2) The patient’s specified alternative location or method of contact.

5. **Decision-Making Authority:** The Clinic or Department Manager, Operations Director, and the Chief Privacy Officer each have final authority to deny requests for more confidential communications.
   a. Denial of Requests: Clinic or Department Managers and Operations Directors may make the decision to deny a request for more confidential communications without input from the Privacy Office. However, if they prefer not to make the decision to deny the request or have a question about the implications of such a decision, the Privacy Office will review the request with the appropriate clinic/department personnel and assist with the decision. Decisions to deny, wherever they are made, must be documented by the person who made the decision.
   b. Only the Chief Privacy Officer may grant requests and approve changes in communication that will affect more than one clinic or area. Any accommodation agreed to by any other staff members is not valid.

B. DEFINITIONS

1. **Verbal Communications:** Includes face-to-face conversations or telephone conversations.

2. **Written Communications:** Includes printed reports, bills, notifications, letters, copies of documents, or any other type of paper correspondence sent or delivered to the patient by any means, including electronically.
SECTION 4: PATIENT’S RIGHTS

4.4. Request for More Confidential Communications (continued)

C. PRIVACY REQUIREMENTS

1. A covered health care provider must permit individuals to request, and must accommodate reasonable requests, to receive communications of PHI from the covered health care provider by alternative means or at alternative locations.

2. A covered entity may require the individual to make a request for a confidential communication in writing.

3. A covered entity may condition the provision of a reasonable accommodation on:
   a. When appropriate, information as to how payment, if any, will be handled; and
   b. Specification of an alternative address or other method of contact.

4. Covered entities may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

D. PROCEDURE

1. Verify Identity and Authority: Make reasonable efforts to verify the identity of a person requesting the restriction, and if not the patient, their relationship to the patient and authority to make the request. (See SECTION 1: General HIPAA and Privacy Rules: Verification of Identity and Authority in this manual.) If a patient or legal representative has documents to corroborate identity or authority, attach copies to the Request form.

2. Provide Assistance: Assist the patient or representative to complete a Request for Special Privacy Protections form. Give the requestor a copy of the completed form.

3. Response Coordination: If a request for More Confidential Communications requires assistance from the Privacy Office, forward the completed Request form to the appropriate Privacy Office as soon as possible. Responses to these referred requests are the responsibility of the Privacy Office.
   a. If the request is denied, the Clinic or Department Manager, the Operations Director, or the Privacy Office will notify the patient of the denial and the reason(s) on the Response to Request for Special Privacy Protections form or in a letter. Place copies of the request and the response in the patient’s health record. (The original documents will be filed in the Privacy Office.)
   b. If the request is granted, the Privacy Office will inform the patient of the terms of the approval on the Response to Request for Special Privacy Protections form or in a letter. Place a copy of the completed Request and Response forms in the patient’s health record. (The original documents will be filed in the Privacy Office.)
      1) Indicate the alternative communication arrangements in the patient’s record.
      2) Notify all staff affected by the communication change to ensure that the request is implemented in operational activities.
      3) Notify your supervisor and/or the Privacy Office immediately if any problems occur as a result of the use of the alternative location or method of communication.
SECTION 4: PATIENT’S RIGHTS

4.4. Request for More Confidential Communications (continued)

4. Termination of Special Protections: If the communication arrangement is terminated or changed, the Privacy Office will provide a copy of the Termination of Special Privacy Protections form to both the patient and the clinic or department. Place the completed Termination form in the patient’s health record.

   a. Make appropriate changes in the chart or other documentation to indicate that the communication arrangement has been terminated.
   
   b. Notify all staff affected by the termination of the confidential communications to ensure that the change is implemented in operational activities.

5. Retain all documentation for at least six years after the date that it was last in effect.

E. REFERENCES

HIPAA: 45 CFR §164.501 Definitions; § 164.522 Right to Request Privacy Protections

F. EXHIBITS:

   Form: Request for Special Privacy Protections

Back to Table of Contents
SECTION 4: PATIENT'S RIGHTS

4.5. Request for Amendment of Records

A. POLICY

1. **Right to Request:** Patients or personal representatives have the right to request that the University of Florida (UF) correct or amend protected health information (PHI) about the patient that is included in a designated record set.

2. **Responding to Requests:** When a patient or authorized representative requests an amendment of the patient’s personal health record, and the author of the documentation agrees with the request, the appropriate amendment should simply be completed by the author, using approved error-correction or other procedures, and without requiring the patient to complete a formal Request for Amendment form or referring the request to the Privacy Office.

3. **Privacy Office Review:** The Privacy Office will review formal written requests for amendments when the author of the documentation in question does not agree with the request to alter the record or in cases where the author is no longer available to act on an amendment request.

4. **Denial of Requests:** If a request for amendment is denied, and the patient chooses to submit a written statement disagreeing with the denial, the statement will be included in the patient’s health record. UF reserves the right to reasonably limit the length of a statement of disagreement from the patient.

B. DEFINITIONS

1. **Addendum:** Entries added to a health record to provide additional information in conjunction with a previous entry. The addendum should be timely, bear the current date, time, and reason for the additional information being added to the health record.

2. **Amendment:** The formal and deliberate alteration of a health record, after the original documentation has been completed and signed by the provider, to make the original documentation more accurate. No individual entries may be altered, obliterated, removed or destroyed.

3. **Correction:** The formal and deliberate alteration or other modification of documentation to make it more accurate. In electronic records, corrections must be made as addendums; they may also involve removing information from one record and posting it to another within the electronic document management system.

4. **Deletion:** The action of permanently eliminating information that is not viewable in a paper record or tracked in a previous version of an electronic record. UF does not allow permanent deletions of clinical information from any health records.

C. PRIVACY REQUIREMENTS

1. **Patient’s Right:** The covered entity must permit an individual to request that the covered entity amend the PHI maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.
SECTION 4: PATIENT’S RIGHTS

4.5. Request for Amendment of Records (continued)

2. **Timely Response:** The covered entity must act on the individual’s request for an amendment no later than 60 days after receipt of such a request.

3. **Response to Requests:** A covered entity may deny a patient’s request for amendment if it is determined that the PHI or record:
   
   a. Was not created by the covered entity, unless the patient provides reasonable evidence that the originator of the PHI is no longer available to act on the request;
   
   b. Is not part of the designated record set;
   
   c. Would not be available for inspection under the right to access; or
   
   d. Is accurate and complete.

**D. PROCEDURES FOR STAFF**

1. **Verify Identity and Authority:** Make reasonable efforts to verify the identity of a person requesting the amendment, and if not the patient, their relationship to the patient and authority to make the request. (See SECTION 1: General HIPAA and Privacy Rules: Verification of Identity and Authority in this manual.) If a patient or legal representative has documents to corroborate identity or authority, attach copies to the Request form.

2. **Provide Assistance:** Notify your supervisor of the request immediately. If directed to do so, assist the patient or representative to complete a Request for Amendment form. Forward the completed Request form to your immediate supervisor.

3. **Follow Up:** After review, the request for amendment will either be denied or granted. Refer all questions about the grant or denial of an amendment request to your supervisor.

**E. PROCEDURES FOR MANAGERS**

1. **Review the Request and Decide How to Act on It:** Identify the scope of the request and the specific PHI affected; then determine what action should be taken and who will need to act on the request. Refer only extraordinary or disputed patient requests for amendments of health information, which will require special arrangements outside the normal course of business, to the Privacy Office.
   
   a. If a request for correction or amendment will be granted and carried out without referral to the Privacy Office, the original Request form with documented response may be filed/scanned into the patient’s health record.
   
   b. If the clinic requests assistance from the Privacy Office, the request will be reviewed with a representative from the clinic or department, the attending practitioner, or the author of the original documentation (if available) to determine if the amendment is warranted.

   1) If, after review, the material in question is deemed accurate and correct, the Privacy Office will notify the patient or representative that the request has been denied and the reason(s).

   2) If, after review, a correction or amendment is deemed reasonable and warranted, and an authorized individual is willing to add an addendum, follow the steps in #2 following:
SECTION 4: PATIENT’S RIGHTS

4.5. Request for Amendment of Records (continued)

2. **Make Corrections:** For corrections of original paper or electronic documentation, the author should use approved error-correction techniques to make the correction.

   a. If the author is no longer available, the patient’s current provider may make a new entry to clarify an incorrect, ambiguous, or unclear entry. No completed entry may be altered or removed.

   b. If the correction is part of a transcribed report, add a note to the electronic report to indicate that a correction has been made. (Contact Shands HIM as needed to obtain the procedure for noting corrections in dictated reports.)

3. **Make an Amendment:** For adding new material to the health record, a supervisor or other designated person should add the additional material to or near the part of the paper record that is affected or scan/upload additional material into the electronic record. Mark the amendment in such a way that it will accompany any future disclosures of the PHI that was amended.

4. **Document the Response to a Request:**

   a. If a request for amendment is granted, document the response on the lower part of the original Request for Amendment form. Either the department manager or the Privacy Office will then:

      1) Notify the patient or representative of the terms of the granted request;

      2) Make reasonable efforts to provide the amendment to persons identified by the requestor.

   b. If a request for amendment or correction is denied:

      1) Either the department manager or the Privacy Office will notify the patient or representative of the reason(s) for the denial on a Response to Request for Amendment form or in a letter.

      2) Place a copy of the form or letter in the patient’s record. Send originals to the Privacy Office.

5. **Future Disclosures:**

   a. Include the patient’s request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI if the patient has requested such action.

   b. Include all written statements of disagreement and subsequent rebuttals, or, at UF’s election, an accurate summary of any such information, with any disclosure of the PHI to which the disagreement relates.

6. **Corrections/Amendments from Other Providers:** If another provider notifies UF of an amendment to a patient’s PHI, UF must amend the PHI in appropriate designated record sets it possesses.

**F. REFERENCES**

HIPAA: 45 CFR §164.501 Definitions; §164.526 Amendment of Protected Health Information

**G. EXHIBITS**

Request for Amendment of a Health Record (Form)
SECTION 4: PATIENT’S RIGHTS

4.6. Privacy Complaints

A. POLICY

1. **Complaint Process:** The University of Florida (UF) has provided a process for individuals to make complaints concerning violations of UF’s privacy policies and procedures. Complaints should be filed in writing, either on paper or electronically, within 180 days of when the patient or representative knew or should have known that a violation had occurred.

2. **Filing a Privacy Complaint:** Patients or their legal representatives may file formal complaints with UF or with the Secretary of Health and Human Services, if they believe the patient’s privacy rights have been violated. UF will document all complaints received, and their disposition.

3. **Complaint Resolution:** UF will investigate and attempt to resolve all complaints relating to breaches of privacy and security of protected health information (PHI) within a reasonable time after a complaint is received.

4. **Non-Retaliation:** UF will not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person filing a complaint or inquiring about how to file a complaint.

5. **No Waiver of Rights:** UF will not require patients to waive their rights to file a privacy complaint as a condition for providing treatment, arranging for payment, enrollment in a health plan, or eligibility for benefits.

B. DEFINITIONS

1. **Complaint:** An allegation of wrongdoing against an individual or organization.

2. **Breach:** An actual violation of policy or procedure; going against established rules.

C. PRIVACY REQUIREMENTS

1. **Filing a Complaint:** A person who believes a covered entity is not complying with the administrative simplification provisions may file a complaint with the Secretary (of Health and Human Services).
   a. A complaint must be filed in writing, either on paper or electronically.
   b. A complaint must name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable administrative simplification provision(s).
   c. A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.
   d. The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

2. **Non-Retaliation:** A covered entity may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for—
   a. Filing of a complaint under the Privacy Rule;
SECTION 4: PATIENT’S RIGHTS

4.6. Privacy Complaints (continued)

b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under the Privacy Rule; or

c. Opposing any act or practice made unlawful by the Privacy Rule, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI.

3. **Contact Person:** A covered entity must designate a contact person or office who is responsible for receiving complaints.

4. **Complaint Process:** A covered entity must provide a process for individuals to make complaints concerning the covered entity’s policies and procedures required by the Privacy Rule or its compliance with such policies and procedures. A covered entity must document all complaints received, and their disposition, if any.

5. **Waiver of Rights:** A covered entity may not require individuals to waive their rights under any part of the Privacy Rule, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

D. **PROCEDURES**

1. **Customer Service:** Encourage any patient or personal representative who indicates a desire to file a privacy complaint to discuss the situation with a supervisory or administrative person first.
   a. Document all conversations concerning the alleged violation of privacy.
   b. Listen and offer apologies, if appropriate, but only for discomfort and/or inconvenience; without acknowledging any wrongdoing.

2. **Provide Assistance:** If the patient wants to file a formal complaint, provide a Privacy Complaint form (see Forms) and assist with completion of the form, if necessary.

3. **Where to File Complaints:**
   a. Any Privacy and/or Security Complaints related to patient information may be directed to the UF Privacy Offices in Gainesville or Jacksonville first:
      1) Chief Privacy Officer, University of Florida, PO Box 113210, Gainesville, FL 32610
         Phone: 352-273-1212, Toll-Free Phone: 866-867-4472(HIPA), E-mail: privacy@ufl.edu
      2) HIPAA Compliance Manager, UF-Jacksonville, 653-1 West 8th St., Jacksonville, FL 32209-6511
         Phone: 904-244-6229, 904-244-2079, Fax: 904-244-3190, E-mail: privacy@ufl.edu
   b. Privacy complaints may also be filed with the Office for Civil Rights: they recommend that you use the OCR Health Information Privacy Complaint Form Package. You can also request a copy of this form from an OCR regional office. If you need help filing a complaint or have a question about the complaint or consent forms, please e-mail OCR at OCRMail@hhs.gov. For more information, see their website: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html
SECTION 4: PATIENT’S RIGHTS

4.6. Privacy Complaints (continued)

4. **Inform and Document:** Inform the UF Chief Privacy Officer (or, in Jacksonville, the HIPAA Compliance Manager) immediately when a complaint is received from a patient or other individual. If the patient does not complete the Complaint Form immediately, collect at a minimum:
   
a. The name and contact information for the complainant;
b. The date and time of the complaint;
c. The name of the staff member who received the complaint.

5. **Follow Up:** The Chief Privacy Officer or designated representative will make every effort to contact the patient or representative within 3 (three) business days of receiving notice of a formal complaint. After investigation of a complaint that directly affects a patient or the complainant, the affected person or representative will be contacted with the results of the investigation and the corrective actions to be taken, if appropriate.

**E. REFERENCES**

HIPAA: 45 CFR §160.306 (Complaints to the Secretary), §164.530(a)(1) Personnel Designations; (d), (g), and (h) Complaints to the Covered Entity

**F. EXHIBITS**

Form: Privacy Complaint

[Back to Table of Contents]
SECTION 4: PATIENT’S RIGHTS

4.7. Accounting for Disclosures

A. POLICY

Background: Patients under the care of the University of Florida (UF) have a right to know what happens to their protected health information (PHI), including with whom the information has been shared, when, and for what reason. Some specific uses and disclosures are included in UF’s Consent for Treatment, which the patient must sign before services are provided, except, of course, in emergency treatment situations. Most other routine uses and disclosures of PHI are described in the Joint Notice of Privacy Practices (see Forms), and, in general, the patient’s permission is obtained before information is disclosed to third parties. There are instances, though, when obtaining authorization is either not possible, not practical, or is not in the patient’s best interests (i.e., suspected child abuse where the child’s parent/guardian is the suspect). However, UF must still be able to account for these disclosures of PHI if asked for them by the patient or representative.

There are three aspects to this Accounting for Disclosures process: 1) the patient’s right to request an accounting and what the patient may expect to receive from the report; 2) UF’s responsibility to record the appropriate disclosures so that an accurate accounting may be provided upon request, and 3) UF’s responsibilities in responding to a request for such an accounting.

1. Patients’ Rights:

a. Patients have the right to receive an accounting of disclosures of PHI made by UF if the disclosures:
   1) Were not related to treatment or health care operations, and
   2) Were not authorized by the patient.

b. Limitations: Patients may request an accounting of disclosures for a period of time up to and including the six years prior to the date on which the accounting is requested. The accounting will not include a list of system users who have accessed the patient’s records during that time period.

c. Fees for providing an accounting report:
   1) The first accounting in any 12-month period will be provided without charge to the requestor.
   2) For each subsequent request by the same individual within any 12-month period, UF may impose a reasonable, cost-based fee. The requestor must be informed in advance and given an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

2. Use of the Online Disclosure Tracking System: UF’s On-Line Disclosure Tracking System (DTS) must be used to record all qualifying disclosures for the purpose of providing a timely accounting if one is requested. The DTS is a university-wide system for recording the limited types of PHI disclosures that must be accounted for if a patient asks for a report.

a. For a list and explanation of qualifying disclosures, please see the Privacy Office website: http://privacy.health.ufl.edu/training/disclosure/index.shtml

b. Only authorized users may access and enter data into the System. Each department, clinic, or other area responsible for any PHI must designate at least one person as an authorized user.
SECTION 4: PATIENT’S RIGHTS

4.7. Accounting for Disclosures (continued)

NOTE: The DTS is **not for reporting incidents** to the Privacy Office. Entering a disclosure in the system **will not notify** the Privacy Office of an incident; an Incident Report must be completed and sent to the Privacy Office for investigation, then, if necessary, a related disclosure may be entered into the DTS.

3. **UF’s Responsibilities:**
   a. The UF Privacy Office will coordinate and respond to all requests for accountings of disclosures. (See **SECTION 2. Responding to Patients’ Rights Requests** in the Privacy Management Manual.)
   b. UF must act on a request for an accounting of disclosures of PHI within 60 days (with the possibility of a 30-day extension, if necessary) after receiving the request in writing.

4. **Temporary Suspension of Right:** UF will temporarily suspend an individual’s right to receive an accounting of disclosures that were made to a health oversight agency or law enforcement official, for the time specified by such agency or official, if such agency or official provides UF with a written statement that such an accounting to the individual would be reasonably likely to impede the agency’s activities and specifying the time for which such a suspension is required.

5. **Accounting for Disclosures during Research.** UF Researchers who disclose PHI to individuals or entities outside of the health care components of UF for any reason are responsible for tracking all such disclosures that were not directly related to treatment or health care operations, and which were not authorized by either the patient or the reviewing IRB.

**B. DEFINITIONS**

1. **Accounting for Disclosures:** A listing of a covered entity’s disclosures of PHI that were made, concerning a specific patient, for purposes other than disclosures needed for treatment and health care operations, disclosures made in response to a valid authorization, and certain other limited disclosures.

2. **Authorized User:** With respect to the Online Disclosure Tracking System, a person designated by their unit to access the system; users obtain and maintain a system log-on and password, enter required data about disclosures, and assist the Privacy Office to respond to requests for accountings of disclosures.

3. **Disclosure:** The release, transfer, provision of access to, or divulging in any manner, of PHI held by UF.

**C. PRIVACY REQUIREMENTS**

1. **Patient’s Right:** An individual has a right to receive an accounting of disclosures of PHI made by a covered entity (CE) in the six years prior to the date on which the accounting is requested, except for disclosures:
   a. To carry out treatment, payment and health care operations;
   b. To individuals of PHI about them;
   c. Incident to a use or disclosure otherwise permitted or required by the Privacy Rule;
SECTION 4: PATIENT’S RIGHTS

4.7. Accounting for Disclosures (continued)

d. Pursuant to a valid authorization;
e. For the facility’s directory or to persons involved in the individual’s care or other notification purposes;
f. For national security or intelligence purposes;
g. To correctional institutions or law enforcement officials),
h. As part of a limited data set; or
i. That occurred prior to the compliance date for the covered entity.

2. **Temporary Suspension of Right:** The CE must temporarily suspend an individual’s right to receive an accounting of disclosures made to a health oversight agency or law enforcement official, for the time specified by such agency or official, if such agency or official provides the CE with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

3. **Information to be tracked for each disclosure includes:**

   a. The date of the disclosure;
   b. The name of the entity or person who received the PHI and, if known, their address;
   c. A brief description of the PHI disclosed; and
   d. The purpose of the disclosure.

4. **Multiple Disclosures:** If, during the period covered by the accounting, the CE has made multiple disclosures of PHI to the same entity for a single purpose, the accounting may provide the information required above for the first disclosure during the accounting period, along with the frequency, periodicity, or number of the disclosures made during the accounting period and the date of the last such disclosure during the accounting period.

5. **Research Disclosures:**

   a. If, during the period covered by the accounting, the CE has made disclosures of PHI for a particular research purpose for 50 or more individuals, the accounting may, with respect to such disclosures for which the PHI about the individual may have been included, provide:

   1) The name of the protocol or other research activity;
   2) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
   3) A brief description of the type of PHI that was disclosed;
   4) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
   5) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
   6) A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.
SECTION 4: PATIENT’S RIGHTS

4.7. Accounting for Disclosures (continued)

b. If the CE provides an accounting for research disclosures, and if it is reasonably likely that the PHI of the individual was disclosed, the CE shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

6. **Provision of an accounting:** The CE must act on the individual’s request for an accounting, no later than 60 days after receipt of such a request, with the possibility of an extension of no more than 30 days, provided that the CE gives the individual a written statement of the reasons for the delay.

7. **Fees for providing an accounting:** The CE must provide the first accounting to an individual in any 12 month period without charge.
   a. The CE may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period.
   b. The CE must inform the individual in advance of the fee and provide the individual with an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

8. **Documentation:** Disclosure tracking information, including copies of requests, copies of accountings provided, and the titles of persons or offices responsible for received and processing requests, must be maintained for at least six years.

D. **PROCEDURES**

1. **Accessing and Using the Online Disclosure Tracking System:** Person(s) designated to enter data into the system complete a short tutorial and a form to apply for a user ID and password. The tutorial, forms and instructions are located on the Privacy website at http://privacy.health.ufl.edu. User ID’s expire automatically after 90 days of non-use, but can be re-activated by contacting the Privacy Office.

2. **Recording Disclosures:** When a disclosure of PHI meeting policy criteria or an accidental or unauthorized disclosure has been discovered, do the following:
   a. Complete an Incident Report to notify the Privacy Office of the disclosure, if appropriate.
   b. When requested to do so by the Privacy Office, record the following types of disclosures in the online Disclosure Tracking System. Follow the detailed instructions in the Disclosure Tracking System User Guide to enter all information requested.

3. **Requesting an Accounting of Disclosures**
   a. Patients or their representatives should submit a request in writing to the Shands Director of Health Information Management or to the UF Physician’s Clinic Manager. The request must include a time period, not longer than six years for the accounting.
   b. If the request is the second (or more) during a 12-month period, notify the Privacy Office first, prior to beginning the process, so that fees can be calculated. Then notify the requestor of the cost of the accounting and give the requestor an opportunity to withdraw or modify the request before any costs are incurred. (The first accounting request within a 12 month period is free of charge.)
SECTION 4: PATIENT’S RIGHTS

4.7. Accounting for Disclosures (continued)

4. Responding to Written Requests for Accounting of Disclosures
   a. Verify the identity of the requestor, and, if not the patient, the relationship of the requestor to the patient, and their authority to receive the accounting.
   b. If any disclosures have been recorded on a paper Tracking Log in the patient’s health record, attach a copy of the Log to the original Request for Accounting, and forward both to the Privacy Office. If there is no Tracking Log in the patient’s health record, send only the Request form. Retain a copy of the request in the patient’s health record.
   c. The Privacy Office will coordinate the response to the request. Maintain a copy of the response, when received, along with the request in the patient’s health record.

E. REFERENCES

HIPAA: 45 CFR § 164.528 (Accounting of Disclosures)

F. EXHIBITS

Form: Request for Accounting of Disclosures

Back to Table of Contents
SECTION 5: SECURITY OF PHI

5.1. Privacy Safeguards

A. POLICY

1. **All Protected Health Information** (PHI) and other restricted data, created, received, maintained, and transmitted by the University of Florida (UF) in all formats, must be secured from unauthorized access at all times, to protect the information from damage, loss, alteration, tampering, and fraudulent use.

2. **Computer Surveillance**: UF and Shands have the capability to track and log access and activities in much of its information and computing environment. All user activity on UF Academic Health Center (AHC) Information and Computing Environment components, including, but not limited to, access through personal computing devices, is subject to review.

3. **Access to electronic PHI** is defined by levels based on users’ roles and responsibilities:
   a. **Workforce**: Health-related colleges, departments, and clinics must define and justify levels of access to PHI for their workforce members relative to their assigned duties and professional “Need to Know”.
   b. **Students**: The Privacy Office, working with the health-related colleges, defines the levels of access to PHI for students and other trainees who require such access for the completion of academic studies.

B. DEFINITIONS

1. **Access**: (for electronic PHI purposes only) means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any information system resource.

2. **Administrative safeguards**: administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s or business associate’s workforce in relation to the protection of that information.

3. **Authentication**: the corroboration that a person is the one claimed.

4. **Availability**: the property that data or information is accessible and useable upon demand by an authorized person.

5. **Information system**: an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

6. **Integrity**: the property that data or information have not been altered or destroyed in an unauthorized manner.

7. **Physical safeguards**: physical measures, policies, and procedures to protect a covered entity’s or business associate’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
SECTION 5: SECURITY OF PHI

5.1. Privacy Safeguards (continued)

8. **Security incident:** the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

9. **Technical safeguards:** the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

C. PRIVACY REQUIREMENTS

1. **Security standards – General rules:** Covered entities and business associates must do the following:
   a. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity or business associate creates, receives, maintains, or transmits.
   b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
   c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule.
   d. Ensure compliance with the HIPAA Privacy and Security Rules by its workforce.

2. **Implementing Safeguards:** A covered entity or business associate must comply with the applicable standards as provided in the HIPAA Security Rule with respect to all electronic PHI. (See: Security Safeguards for Electronic Records in the HIPAA Privacy Management manual. Also see SPICE: Security Program for the Information and Computing Environment on the UF Health IT website.)

3. **Information access management:** Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of the HIPAA Security Rule.

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. 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 cabinet 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 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.
SECTION 5: SECURITY OF PHI

5.1. Privacy Safeguards (continued)

b. Securing Electronic Records

1) To prevent unauthorized use or disclosure, place computers, monitors, and similar data storage and display devices in areas that limit viewing and prevent access by unauthorized persons; position electronic displays away from public view or shield the viewing screen.

2) Practitioners who access PHI at home or in other non-work locations are expected to use physical safeguards to prevent family members, roommates, and friends from unauthorized viewing of records.

3) Encrypt all PHI stored on removable electronic storage media (cards, CD’s, flash devices, etc.).

4) 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 place in a locked storage unit for secure controlled destruction later.

5) Electronically purge data devices used to store PHI before they are discarded or otherwise taken out of UF’s control.

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 to the Privacy Office immediately.

1) Report known and suspected security incidents to the appropriate Information Security Officer 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. Termination: When an employee terminates employment, collect keys and other access devices if the employee’s job duties included authorized access to any area where PHI is stored or used.

d. Required Training: All workforce members in UF’s health care components complete privacy and security training at orientation and annually.

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.
SECTION 5: SECURITY OF PHI

5.1. Privacy Safeguards (continued)

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. 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 2: Health Information Management: Record Custodians List in this manual.)

1) For Employees:
   a) Electronic Medical Record Access: Route all employee (UF or Shands) requests for access to the current electronic medical record (EMR) system and other UF or Shands health-related computer systems to Shands HealthCare Identity and Access Management.
   b) Electronic Dental Record Access: Route all employee requests for access to the current electronic dental record system to the College of Dentistry IT System Administrator.

2) For Students: Colleges and other units requesting access to the current electronic medical record (EMR) system for their students should direct the requests to the UF Privacy Office for review and approval.
   a) If the student needs access to medical records for a class and will receive some form of academic credit for the work, see SECTION 6: Other Procedures - Student Data Access in this manual for required procedures.
   b) If the student is employed and needs access to medical records for assigned job duties, follow the procedure above for employees.

3) Volunteers: Currently, personal access accounts for the electronic medical record system are not provided to volunteers.

c. Maintaining Access to PHI:
   1) Managers, supervisors, and proctors: Monitor use of computers and electronic information by workforce members, including students. Train all users concerning authorized and appropriate activities; intervene when necessary to protect information and systems.
   2) Individual users: ensure personal compliance with all the rules of use that were agreed to as a condition of gaining access to the information system(s).

d. Terminating Access to PHI:
   1) Managers, supervisors, and proctors:
      a) Monitor needs for access to PHI in all formats by workforce members so that access is not continued beyond the actual need.
SECTION 5: SECURITY OF PHI

5.1. Privacy Safeguards (continued)

    b) Notify Shands HealthCare Identity and Access Management immediately when an employee terminates employment so that access to electronic data systems may be terminated.

    2) Account managers: Terminate access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by UF Health Science Center policies.

E. REFERENCES

1. HIPAA: 45CFR §164.306(a) Security standards: General rules; 164.308 Administrative safeguards: (a)(3) Workforce Security; (a)(4) Information Access Management; (a)(5)(i) Security awareness and training; §164.514(d) Minimum necessary requirements; §164.530 Administrative Requirements: Safeguards (b) Training; (e) Sanctions

2. UF Policies: Acceptable Use Policy, UF Information Technology Security Policies

F. EXHIBITS

None

Back to Table of Contents
SECTION 5: SECURITY OF PHI

5.2. Personal Portable Data Devices / Mobile Devices

A. POLICY

1. **Responsibility**: All University of Florida (UF) faculty, staff, students, and volunteers are responsible for maintaining the confidentiality of all health information (not just protected health information (PHI)), personal identification information (PII), and other restricted data, stored on or transmitted through personal portable data devices, also known as mobile devices, from improper use or disclosure.
   
a. Persons violating this policy may be subject to disciplinary action by UF, up to and including, termination of their relationship with UF and/or denial of future access to a UF information system.
   
b. Persons violating this policy may also be held personally liable for resulting damages and civil or criminal charges. When appropriate, law enforcement, the Department of Health & Human Services (HHS), and/or applicable licensing boards will be notified of incidents.

2. **Devices** include, but are not limited to: wireless/cell phones, “smart” phones of all brands, personal data assistants of all brands, laptops, netbooks, or notebook computers, dictation equipment, digital cameras, video recorders, USB flash/jump drives, memory cards, discs, and tapes, and similar devices.

3. **Security** of protected health information (PHI) and other restricted data accessed, used, stored in, or transmitted through portable electronic devices is subject to the policies of the UF Information Security programs, UF Health Information Security programs, and the provisions of relevant state and federal laws. Disclosure of unsecured PHI or patient data, including images, via electronic devices is strictly prohibited. Unauthorized use or disclosure of PHI or other restricted data via any electronic device will be cause for disciplinary action.
   
a. All devices used to communicate PHI, PII, or other restricted data in any format must be encrypted using approved software that specifically offers HIPAA-compliant access to current electronic health record systems as well as HIPAA-compliant text, data, and image-sharing.
   
b. All devices used to communicate PHI, PII, or other restricted data in any format must utilize approved and encrypted communication channels to transmit the information.

4. **Loss or theft** of portable data devices on which PHI or other restricted data is stored must be reported to the Privacy Office as well as to the University Police Department, whether the device is the property of UF or not.

5. **Use of Personal Devices and Cameras**: Use by workforce members of personal portable data devices that create, store, or transmit text, data, or still or moving images is generally prohibited for work-related purposes in patient care areas, except for the direct provision of patient care and/or during emergencies or disasters. Users are responsible for any activity originating from personal devices.
   
a. Users sharing and receiving photos of PHI must have a professional need to know the information used or shared for treatment purposes.
   
b. Communications and/or images used for healthcare decision making or to provision clinical treatment must become part of the patient’s health record and are subject to record creation and retention requirements.
SECTION 5: SECURITY OF PHI

5.2. Personal Portable Data Devices / Mobile Devices (continued)

c. Examples of acceptable and unacceptable uses of Personal Devices

1) **Acceptable** Uses:
   a) A resident physician photographs a patient’s wound and sends the image to attending physician for consultation.
   b) A nurse “texts” stat lab results to the ordering physician.
   c) A clinician photographs the placement of a healthcare device, excluding any patient identifiers, and sends the image to the device manufacturer for advice.

2) **Unacceptable** Uses:
   a) Patient images recorded out of curiosity
   b) Taking a picture with a patient, at the patient’s request, in a patient care area, and then forwarding the picture to the patient and/or posting the picture on a Facebook page.
   c) PHI shared outside the ufl.edu domain under the assumption of “general healthcare education.”
   d) Auto-forwarding e-mail to any e-mail system outside the ufl.edu domain, such as G-mail, Yahoo, AOL, or similar external e-mail systems.

6. **User Permissions for Communicating PHI**
   a. Clinicians and Employees: Use shall be consistent with the approved purposes of the direct provision of patient care and/or during emergencies or disasters
   b. Students: Use shall be consistent with supervised participation in a clinically affiliated educational program, either through a UF college, or another affiliated college (through an educational agreement) during on-site practicums.

7. **User Protocols and Etiquette:** Disruptive use of IT resources is not permitted. Occasional personal use of IT resources by employees is permitted when it does not consume a significant amount of those resources, is otherwise in compliance with this policy, and meets with the approval of the supervisor.

B. **DEFINITIONS**

1. **Breach (HIPAA):** the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.

2. **Encryption:** the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key (e.g., the translation of data into a secret code).

3. **Health Information:** any information, including genetic information, whether spoken or recorded in any form 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
SECTION 5: SECURITY OF PHI

5.2. Personal Portable Data Devices / Mobile Devices (continued)

b. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

4. **Personal Portable Data Device**: Any easily mobile, usually hand-held, device that provides creation, manipulation, transmission, storage, and/or retrieval capabilities for information, sound, text, or images for personal or business purposes.

5. **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.

6. **Unsecured PHI**: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary [of Health and Human Services].

7. **Workforce**: employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

C. **PRIVACY REQUIREMENTS**

1. **Security standards: General rules.** Covered entities and business associates must do the following:
   a. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity or business associate creates, receives, maintains, or transmits.
   b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
   c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
   d. Ensure compliance with the Security Rule by its workforce.

2. **Administrative safeguards**: Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

D. **PROCEDURES**

1. **Training**: Complete the Mobile Device Privacy and Security Training

2. **Protect Contents**: Use all available measures to protect data stored on or transmitted through portable data devices, including, but not limited to:
SECTION 5: SECURITY OF PHI

5.2. Personal Portable Data Devices / Mobile Devices (continued)

a. **Know your device:** Equipment that only transmits data without storing needs a different level of protection than equipment that also stores data, which will require more security.

b. **Use Proper Authentication Practices and Password Protection:** Use strong passwords; do not share passwords.
   1) Configure the Mobile Device to require a strong password, consistent with or exceeding UF password requirements and to allow no more than ten (10) failed password entry attempts before the device auto-locks.
   2) Configure the device with an inactivity timeout of not more than 10 minutes, which requires re-authentication before use.

c. **Use Encryption Programming and Maintain It:** Download and use only approved software to communicate and protect PHI, PII, or other restricted data during transmission over any wireless network and any non-UF wired network.
   1) Contact the UF and/or AHC IT departments with any questions regarding approved software.
      Update virus protection and malicious software detection and removal products as often as recommended.
   2) An exception to this encryption requirement would only be for specific uses where no restricted data of any type will be stored and encryption would interfere with the device's intended use.

3. **Single User / Single Use:** Limit use of the device to one person and one purpose, either work or personal, but not both. Do not allow friends, family members or children to use or play with a device designated for work purposes.

4. **Limit Data:** Store only the “minimum necessary” data on portable devices. Destroy stored data immediately when information is no longer needed; purge, overwrite, or degauss equipment when ownership changes.

5. **Label Devices:** Place an engraved, electronic, or otherwise indelible label with the owner’s name and contact information sufficient to facilitate return on all portable data devices.

6. **Secure Devices:** Employ other reasonable safeguards as necessary to prevent theft of the device and/or unauthorized viewing of PHI.
   a. Use tracking and recovery software whenever possible.
   b. When not in use, turn the device off and store it in a locked or otherwise secure area.
   c. Do not leave data devices unattended in personal vehicles!

7. **Ensure Proper Disposal of Devices:** Contact the UF or AHC IT Security Department or place a Computer-Related IT Service Request to prepare mobile computing and storage devices for disposal in compliance with Information Security Electronic Media Control, Disposal and Reuse policies.
SECTION 5: SECURITY OF PHI

5.2. Personal Portable Data Devices / Mobile Devices (continued)

8. **Report Loss or Theft:** Notify your immediate supervisor and the following units immediately concerning the loss or theft of a personal data device used for UF business that included PHI, PII, or other restricted data, whether it belonged to UF or not:

   a. UF Privacy Office
   b. UF or AHC IT Security Office
   c. UF Police Department

E. **REFERENCES**

   **HIPAA:** 45 CFR §164.302 Security Standards, §164.308 Administrative safeguards; §164.312 Technical Safeguards; § 164.402 Definitions.

F. **EXHIBITS**

   None

[Back to Table of Contents]
SECTION 5: SECURITY OF PHI

5.3. Electronic Databases

A. POLICY

1. **Requirements:** Any electronic database containing Protected Health Information (PHI), Personal Information, or other restricted data, maintained by any member of the University of Florida (UF) workforce must meet the following conditions:
   a. **Location:** The database must be stored on a secure server, not on a hard drive of any computer, and protected with all security measures required by the IT Security policies and standards, including but not limited to:
      1) Procedures for permitting and authenticating access, and for logging and periodically monitoring access to the database;
      2) Procedures for terminating access for individuals who are no longer associated with the work for which the database was developed;
      3) Processes for backing up the database files and securely storing the back-ups.
   b. **Limited Access:** Access to the database must be limited:
      1) By password-protected personal accounts assigned to specifically identified individuals who are authenticated by the custodian of the database,
      2) To defined work-related purposes and for defined periods of time.
   c. **Access Logs:** A log of individuals who have been given access to the database must be maintained, and should include, at a minimum:
      1) The individual’s name and UF Identification number;
      2) The date access was given and the reason access was given to the database;
      3) The individual’s assigned account information, except password;
      4) The date access was terminated and the reason for termination.

2. **Products of Electronic Databases:** Paper or hard-copy print-outs or components of electronic databases, which contain PHI or other restricted data, must be stored in lockable, non-portable units, such as filing cabinets, suitable for the format of the database and located in an approved storage area.

3. **Transport of Data:** Any data copied, downloaded, or otherwise moved from the main electronic database onto portable electronic media or devices must be properly encrypted or de-identified.

4. **Purging and Destruction:** The data, including all copies and print-outs of the data, must be properly destroyed when no longer needed. Identifiable personal and patient information may not be removed from UF premises in formats that would allow for easy access by unauthorized persons.

B. DEFINITIONS

1. **Back-up:** Copy of electronic files and applications made to avoid loss of data and facilitate recovery of data and information.

2. **Database:** A collection of information, usually recorded in alpha or numeric terms, and organized for rapid search and retrieval, as by a computer.
SECTION 5: SECURITY OF PHI

5.3. Electronic Databases (continued)

3. **Encryption**: The use of an algorithmic process to transform electronic data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

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. **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.

C. **PRIVACY REQUIREMENTS**

1. **Ensure** the confidentiality, integrity, and availability of all electronic PHI the covered entity creates, receives, maintains, or transmits.

2. **Protect** against any reasonably anticipated threats or hazards to the security or integrity of such information, and against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.

D. **PROCEDURES**

1. Review all plans for electronic databases with your department’s Security Manager. A formal security review is required for new databases.

2. If the database is for research-related data, also review the security measures for the database with the appropriate IRB.

E. **REFERENCES**

1. **HIPAA**: 45 CFR §164.306 (Security standards: General rules), §164.308 (Administrative safeguards).

2. **Florida Statutes**: 501.171(g) (Security of confidential personal information)

3. **UF HSC SPICE Policies and Standards**: [http://security.health.ufl.edu/isa_ism/policies.shtml](http://security.health.ufl.edu/isa_ism/policies.shtml)

F. **EXHIBITS**

None
SECTION 5: SECURITY OF PHI

5.4. Electronic Mail

A. POLICY

1. **Application:** E-mail may be used by University of Florida (UF) workforce members to transmit Protected Health Information (PHI) and other restricted data, except Social Security Numbers, under specific conditions and for limited purposes.

2. **The Minimum Necessary Rule** applies to all e-mail that includes PHI.

3. **Scope:** This policy applies to all use of electronic mail systems within UF where the correspondence contains PHI and either originates from or is forwarded into a computer or network used for UF mission or business purposes. It applies to all e-mail users including, but not limited to, faculty, staff, students, and volunteers.

4. **Conditions:** All applicable conditions below must be met in order to use PHI in e-mails:

   a. **Patients and Research Participants:** PHI may be included in e-mails between clinicians and patients or between researchers and subjects only if the patient/subject has signed an Authorization for Correspondence via Electronic Mail. (See Forms)
      1) E-mail should only be used in cases where the patient does not have access to an alternative secure electronic communications portal, such as one associated with UF’s electronic health record system.
      2) When replying to e-mail containing PHI or other types of restricted data from patients/senders outside the ufl.edu system, the restricted data may not be re-sent in the e-mail reply; that is, the response from UF may not contain the restricted data that was included in the sender’s original e-mail. PHI may be re-sent if the patient who is the subject of the PHI, or the patient’s legal representative, has signed an E-mail Authorization.
      3) Clinically relevant e-mail messages between patients and caregivers must be printed in full and included in the patient’s health record.

   b. **Staff-to-Staff:** PHI may be included in e-mails between and among clinicians, researchers, and support staff only for the following purposes:
      1) Making Appointments / Referrals
      2) Billing Inquiries
      3) Requesting Consultations
      4) Prescription Refills

   c. **Internal E-mails:** E-mails meeting the above conditions and containing PHI or other restricted data may only be sent from one ufl.edu address to another ufl.edu address. The sender of any such e-mail is responsible for ensuring that the recipient’s address is within the ufl.edu e-mail system.
      1) UF business-related e-mail may not be auto-forwarded or otherwise transferred to non-ufl.edu accounts, including but not limited to, e-mail services such as Gmail, Yahoo, Hotmail, etc.
      2) No distribution lists, personal e-mail groups, or other multi-recipient lists may be used to send e-mail that contains PHI or other restricted data.
      3) Access to ufl.edu e-mail accounts through the Internet must be by secure (SSL) connections.
SECTION 5: SECURITY OF PHI

5.4. Electronic Mail (continued)

d. **Research Communications:** PHI may be included in e-mails between and among researchers, staff, and authorized third parties, but only as a password-protected attachment file.

e. **External E-mails:** Authorized external e-mail communications containing PHI or other restricted data (i.e., sent outside the ufl.edu domain) must be protected by encryption. Encryption may be accomplished in either of the following ways:

1) The connection(s) between the sender and the receiver is encrypted (i.e. through SSL, TLS or VPN), or

2) The data is placed in a file, the file is encrypted and the pass-code used to decrypt the file is communicated to the recipient in a secure fashion. DO NOT include the pass-code in the e-mail with the file.

**B. DEFINITIONS**

1. **E-mail:** A means or system for transmitting written messages electronically (as between terminals linked by telephone lines, cable networks, or other relays).

2. **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.

3. **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.

**C. PRIVACY REQUIREMENTS**

1. **Patient Rights:** Patients have the right to request communication by alternative means; however, UF is not obligated to agree to the request.

2. **Security:** PHI must be safeguarded against unauthorized use or disclosure at all times.

**D. PROCEDURES**

1. **Patient Communications:** Encourage patients who want to communicate electronically with caregivers about healthcare issues to use the on-line communications portal associated with UF’s current electronic health record system.
SECTION 5: SECURITY OF PHI

5.4. Electronic Mail (continued)

2. **Alerting Patients and Research Subjects of E-mail Hazards:** Address all of the following issues with patients/subjects or personal representatives who want to communicate by e-mail, before they sign an authorization. Provide a copy of the Alert for Electronic Communications tip-sheet to the patient (see Forms).
   a. E-mail at UF can be forwarded, intercepted, printed and stored by others.
   b. E-mail communication is a convenience and not appropriate for emergencies or time-sensitive issues.
   c. Highly sensitive health or Personal Information should not be communicated by e-mail (i.e., HIV status, mental illness, chemical dependency, worker compensation issues, financial account information, Social Security numbers, etc.)
   d. Employers generally have the right to access any e-mail received or sent by a person at work.
   e. Staff other than the health care provider may read and process e-mail.
   f. Clinically relevant messages and responses will be documented in the patient’s health record.
   g. Communication guidelines must be defined between the clinician/researcher and the patient/subject, including,
      1) How often e-mail will be checked,
      2) Instructions for when and how to escalate to phone calls and office visits, and
      3) Types of transactions appropriate for e-mail.
   h. E-mail message content must include:
      1) The subject of the message in the subject line, i.e., Prescription Refill, Appointment Request, etc., and
      2) Clear patient/subject identification including name, telephone number and record identification number in the body of the message.
   i. UF will not be liable for information lost or misdirected due to technical errors or failures.

3. **Retain** the completed Authorization form in either the patient/subject’s health record or a separate file maintained by the clinician/researcher. Give a completed copy to the patient, if necessary.

4. **E-mail Disclaimer Notice:** Include the following or a similar confidentiality disclaimer statement in all e-mails that are sent from UF:

   NOTE: This communication may contain information that is legally protected from unauthorized disclosure. If you are not the intended recipient, please note that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, you should notify the sender immediately by telephone or by return e-mail and delete this message from your computer.
SECTION 5: SECURITY OF PHI

5.4. Electronic Mail (continued)

E. REFERENCES

1. HIPAA: 45 CFR §164.306 Security standards: General rules, §164.522 Right to Request Privacy Protections

2. Florida Statutes: 501.171(g) (Security of confidential personal information)

3. UF Regulations: https://wiki.helpdesk.ufl.edu/AccountsResources/HowDoIPasswordMyGatorLinkEmail

F. EXHIBITS

1. Alert for Electronic Communications

2. Authorization for Electronic Communications

Back to Table of Contents
SECTION 5: SECURITY OF PHI

5.5. Video- and Audio-Conferences

A. POLICY

1. **Pre-Approval Required**: Video- and audio-conference programs and services involving the use or disclosure of Protected Health Information (PHI) and initiated by University of Florida (UF) providers or researchers must be reviewed and approved by the Chief Privacy Officer and the Information Security Officer prior to transmission.

2. **Conference Elements for Approval**: The following items must be defined and approved prior to initiating electronic conferencing systems:
   a. Security of transmissions, including adequacy of privacy and security at both the point of initiation and point of reception, transmission modes, and network security.
   b. Compliance with interstate and international privacy laws, as appropriate.
   c. Initiation of a Business Associate Agreement with any service provider, as appropriate.

3. **Patient Rights**: Patients, whose PHI will be shared, and/or their personal representatives, must be given time to review the Alert for Electronic Communications and ask questions, and must sign an Authorization to Use or Disclose PHI via Electronic Means prior to the conference. If the transmissions will be recorded for later use in teaching, this potential use must be included in the authorization.

4. **Personal Communications**: Video- and audio-conferencing as described in this policy are not intended to include communications between patients and providers (or subjects and researchers) using a personal account on a commercial Internet telephony service with or without a video component (i.e., Skype, Google Talk, Yahoo! Messenger, Facebook Video, etc.). However, these types of communication also require that the patient be directed to review the Alert for Electronic Communications and sign an authorization for use and disclosure of PHI.

B. DEFINITIONS

1. **Video-conference**: A meeting among persons where real-time sound and image transmission technologies are utilized simultaneously. Communication is multi-way and synchronous, as it would be if all parties were in the same room; also known as teleconferencing and tele-health or tele-medicine.

2. **Audio-conference**: Real-time verbal communications over distances, using electronic sound transmission systems, between two or more persons.

C. PRIVACY REQUIREMENTS

1. **Business associate includes**: A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a covered entity and that requires access on a routine basis to such PHI.

2. **General requirements**: Covered entities and business associates must do the following:
   a. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity or business associate creates, receives, maintains, or transmits.
SECTION 5: SECURITY OF PHI

5.5. Video- and Audio-Conferences (continued)

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

D. PROCEDURES

Discuss all plans for video- or audio-conferences that will involve PHI with the Chief Privacy Officer and the appropriate Security Officer.

E. REFERENCES

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

F. EXHIBITS

Form: Authorization to Use or Disclose PHI via Electronic Means
Alert for Electronic Communications

Back to Table of Contents
SECTION 5: SECURITY OF PHI

5.6. Verbal, Telephone, and Other Types of Communications

A. POLICY

1. **Communications**: The University of Florida (UF) will use verbal and other means (interpreters, sign language, written notes, etc.) to communicate protected health information (PHI) as necessary for treatment, payment, and health care operations, in accordance with applicable federal and state laws.

2. **Use of Interpreters**: The patient’s authorization is not required for use of an interpreter if the patient speaks a language other than English or is hearing impaired, and the provider uses the interpreter to communicate about treatment, payment or health care operations. The following conditions apply:
   a. *UF may use an organization or individual* as a business associate to perform interpreter services on its behalf, including private commercial companies, community-based organizations, or telephone interpreter service lines. A valid Business Associate Agreement is required.
   b. *UF may use a member of UF’s workforce* (i.e., a bilingual employee, a contract interpreter on staff, or a volunteer), as long as the employee has completed HIPAA training and signed a Confidentiality Statement and the patient agrees to the arrangement.
   c. *UF may communicate with a patient through the patient’s family member, close friend, or other person identified or approved by the patient to serve as his or her interpreter for a healthcare encounter.* That interpreter is not considered a business associate of the health care provider.
   d. The health care provider may obtain the patient’s agreement to the use of an interpreter either in writing or verbally, or the provider may reasonably infer, based on professional judgment and the circumstances, that the patient does not object to the disclosure of PHI to the interpreter.

3. **Use of Telecommunication Devices for the Hearing Impaired**
   a. *Telecommunications Relay Services (TRS):* The TRS is a public service, available without cost to all persons and businesses, none of whom need to employ, contract with or otherwise establish business relationships with the TRS. When performing services for a covered entity, the TRS is not acting for or on behalf of the covered entity and is not the covered entity’s business associate.
   b. When a covered health care provider initiates a call using the TRS without the individual’s prior agreement, the individual must be given an opportunity to agree or object to disclosures of PHI to a TRS Call Assistant (CA) so that pertinent information can be shared during the telephone communication. (See 45 CFR §164.510(b))

B. DEFINITIONS

1. **Interpreter**: One who translates from one language into another, usually orally, but also by hand-signs.
2. **Sign Language**: A formal or informal system of manual, facial, and other body movements as the means of communication, especially among deaf people.
3. **Verbal Communications**: Includes all types of oral and assisted communications where the intent is to carry on a dialogue between one or more persons.
SECTION 5: SECURITY OF PHI

5.6. Verbal, Telephone, and Other Types of Communications (continued)

C. PRIVACY REQUIREMENTS

1. Security – General Rules: Covered entities and business associates must do the following:
   a. Ensure the confidentiality, integrity, and availability of all electronic protected health information
      the covered entity or business associate creates, receives, maintains, or transmits.
   b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such
      information.
   c. Protect against any reasonably anticipated uses or disclosures of such information that are not
      permitted or required under the Privacy Rule.

2. Family Members and Friends: A covered entity may disclose to a family member, other relative, or a
   close personal friend of the individual, or any other person identified by the individual, the PHI directly
   relevant to such person’s involvement with the individual’s health care or payment related to the
   individual’s health care.

3. Individual’s Right: If the individual is present for, or otherwise available prior to, a use or disclosure
   permitted by 2. above and has the capacity to make health care decisions, the covered entity may use
   or disclose the PHI if it:
   a. Obtains the individual’s agreement;
   b. Provides the individual with the opportunity to object to the disclosure, and the individual does not
      express an objection; or
   c. Reasonably infers from the circumstances, based on the exercise of professional judgment that the
      individual does not object to the disclosure.

4. Minimum necessary applies: When using or disclosing PHI, a covered entity or business associate must
   make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of
   the use or disclosure.

D. PROCEDURES

1. Verbal and Substitute Communications in Healthcare Areas
   a. Speak quietly when discussing a patient’s PHI and avoid the use of patients’ names or other
      identifiers in conversations whenever possible.
   b. Do not discuss PHI in public areas, either verbally or by sign-language; move to private areas for
      exchange of private information.

2. Telephone Use in Healthcare Areas
   a. Conduct telephone conversations that include PHI in private areas, if possible.
SECTION 5: SECURITY OF PHI

5.6. Verbal, Telephone, and Other Types of Communications (continued)

b. *Make reasonable efforts to verify the identity* of the other person(s) before proceeding with a telephone conversation, using departmental procedures or the verification guidelines in this manual (see *SECTION 1: General HIPAA and Privacy Rules: Verification of Identify and Authority* in this manual).

c. **Answering Machines:** It is sometimes necessary to leave a message for a patient who is not at home or cannot come to the phone.
   1) Never leave PHI in a message (diagnoses, lab test names or lab results, surgical procedures, etc.) on an answering machine, voicemail system, or with an unknown person who takes a message for a patient.
   2) When leaving a message is necessary and appropriate, provide enough information to be useful to the patient:
      a) Your name and the name of the care giver;
      b) The generic location: “University of Florida Physicians Clinic” and a call-back number;
      c) What the call is about: an appointment time and date reminder, a needed change in an appointment, insurance question, etc.;

3. **Sharing PHI with a family member or friend** of the patient for purposes of interpretation, see the procedures in *SECTION 3: Uses and Disclosures: Family Members and Friends* in this manual.

4. **Using Interpreters:** Use an interpreter as needed to both work out an agreement for the use of the interpreter, and to share PHI for the healthcare encounter. Document the name of the interpreter or company, the relationship of the interpreter (business associate, volunteer, family member, etc.) and the patient’s agreement in the patient’s record.

**E. REFERENCES**

HIPAA: 45 CFR §164.306(a) Security standards: General rules, §164.502(b) Minimum Necessary, §164.510(b) Uses and Disclosures for Involvement in an Individual’s Care

**F. EXHIBITS**

None

[Back to Table of Contents]
SECTION 5: SECURITY OF PHI

5.7. Faxing Protected Health Information

A. POLICY

1. Facsimile (fax) messages containing protected health information (PHI) or other restricted data may be sent to locations where the physical security and monitoring practices of the receiving fax machine are known or can reasonably be verified.

2. Scope: This policy applies to all facsimile machines used at the University of Florida (UF) where documents containing PHI or other restricted data either originate from, or are received into UF. It applies to all users including, but not limited to, faculty, staff, students, and volunteers.

3. Faxed messages that include PHI, sent from within UF to incorrect recipients outside of UF generally constitute a breach of PHI; such incidents must be reported to the Privacy Office so that the patient whose PHI was disclosed can be notified in accordance with federal regulations.

B. DEFINITIONS

1. Confidentiality Disclaimer: A statement on a fax cover sheet that notifies the recipient of the protected nature of the faxed materials; also informs an unintended recipient how to report a misdirected fax and the consequences of misusing the materials received. A fax disclaimer should include four elements:
   a. That the information is privileged or confidential;
   b. That it is intended for use only by the addressee;
   c. That use of the information is strictly prohibited;
   d. To please notify the sender of the erroneous receipt

2. Fax: A means or system for transmitting copies of documents electronically, usually between terminals linked by telecommunications networks.

C. PRIVACY REQUIREMENTS

1. Security – General Rules: Covered entities and business associates must do the following:
   a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
   b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
   c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.

2. Minimum necessary applies: When using or disclosing PHI, a covered entity or business associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure.
SECTION 5: SECURITY OF PHI

5.7. Faxing Protected Health Information (continued)

D. PROCEDURES

1. Pre-program fax numbers whenever possible. Test the programmed numbers periodically (at least annually) for accuracy, i.e., send a cover sheet and verify by phone, e-mail, return fax, or in person that it was received.

2. Use Cover Sheets: Always use an approved cover sheet form that includes an appropriate confidentiality disclaimer for facsimile messages that contain PHI or restricted data (see Forms). Example of a fax disclaimer statement:

   This facsimile transmission contains information that is confidential and/or protected by law. This information is intended for use only by the addressee indicated above. If you are not the intended recipient, please be advised that any disclosure, copying, distribution, or use of the contents of this information is strictly prohibited. Please call us at the number above to notify us of a fax received in error. Your cooperation is appreciated.

3. Use Verification Procedures: Faxes sent to unknown or unfamiliar locations should be phone-verified before any PHI is transmitted. That is, send the cover sheet alone and then call or otherwise communicate to verify that the intended and authorized person received it and is standing by to receive the PHI documents that will follow, then fax the rest of the materials.

4. Report Faxing Errors: Report misdirected faxes containing PHI or other restricted data to the Privacy Office if the fax is sent to locations outside of UF’s health care components.
   a. In general, misdirected faxes that arrive in UF health care components, whether the fax originated inside or outside of UF, should simply be destroyed and the sender notified. However, there are times when these errors should be reported to the Privacy Office for follow-up:
      1) Multiple misdirected faxes continue to arrive from the same sender, even after being notified of their error.
      2) The contents of the faxes include “super-confidential” patient information.
   b. Misdirected faxes that originate from within UF, but are received by someone outside of UF (private businesses, personal home faxes, etc.), are usually discovered when they are reported by the recipients. Always ask that the materials received in error be either destroyed or mailed back to UF, if the recipient is willing. Complete an Incident Report for these errors and include a copy of the faxed materials that were misdirected.

E. REFERENCES

HIPAA: 45 CFR §164.306(a) Security standards: General rules, §164.312 Technical Safeguards, §164.502(b) Minimum Necessary

F. EXHIBITS:

Form: Fax Cover Page Example

Back to Table of Contents
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.1. Visitors, Vendors, Volunteers and Observers

A. POLICY

1. Any person, invited or otherwise authorized to enter University of Florida (UF) patient-care areas or to view patient care in any UF location, who is not formally associated with one of UF’s healthcare components, must be accounted for either by a formal registration process in the appropriate college, location, or system, or a more informal approval process for short-term shadowing/observing. Such visitors must be accompanied and/or supervised by a UF representative from the patient care area or location at all times. The UF representative is responsible for the actions of the visitor, including any direct or indirect access to protected health information ( PHI).
   a. This policy includes, but is not limited to:
      1) Visiting and volunteering health care professionals,
      2) All visiting students (including UF students enrolled in non-HSC programs),
      3) UF HSC students approved as long-term (up to 12 months) volunteers,
      4) Applicants for UF positions who will be touring patient care areas,
      5) Trade representatives not registered in Rep-Trax (Shands System),
      6) Family members or friends visiting UF employees in their health care workplaces,
      7) Any other similar persons or groups who may directly or indirectly encounter PHI.
   b. This policy does not include:
      1) Observation/Shadowing for 21 days or less by UF students who are enrolled in a UF Health Science Center College or Program,
      2) Fellows, interns, residents, and other students on formal clinical or contractual rotations,
      3) College of Medicine (in session) Medical Students
      4) Students enrolled in UF courses that require physician shadowing hours for graduation
      5) Medical students enrolled in the Medical Student Research Program (MSRP)
      6) Vendors and Trade Reps registered in RepTrax (Shands System)
      7) Courtesy Appointments active in PeopleSoft
      8) Site Monitors for IRB-approved clinical trials
      9) Approved Internships (either through a UF program or as required for graduation)
      10) High School Students enrolled in official UF- and/or HSC-sponsored programs
      11) Patients, or family members or friends visiting or accompanying patients.
      12) Individuals desiring to shadow a Shands employee or volunteering to work in a Shands facility under the supervision of a Shands sponsor; such individuals must apply through the Shands Privacy Office or Shands Volunteer Services.

2. Visiting faculty and applicants for faculty positions who visit one time for less than two days are not required to complete the HIPAA training modules, but are requested to review the UF Health Information Policy and sign the UF Confidentiality Statement prior to beginning activities with UF.
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.1. Visitors, Vendors, Volunteers and Observers (continued)

3. **Required Training:** Vendors, Volunteers and Observers must complete appropriate HIPAA and Privacy Training and sign a Confidentiality Statement prior to beginning activities at UF. Returning Vendors, Volunteers and Observers must renew their HIPAA training annually or as otherwise required.

4. **Minors:** Visitors under 18 years of age and not enrolled in a UF or UF-affiliated student program are prohibited from observing or shadowing in direct patient care areas where protection of the patient’s physical privacy is generally expected. **Where no other exemptions apply** a minor (under 18 years) approved for observing / shadowing must have:
   a. Written permission for the activities from a parent or legal guardian, and
   b. **Written approval by the Dean of the college or a designee.**

5. **Sponsors for Volunteering and Observing:**
   a. UF does not provide any sponsor-matching services for individuals wishing to shadow a health care professional or to volunteer. All arrangements for sponsorship must be made by the individual.
   b. Faculty and staff who sponsor Volunteers and Observers assume full responsibility for their supervision and agree to ensure that they comply with all policies and procedures of the University of Florida (and Shands, if applicable) and all applicable state and federal laws while engaged in activities at UF.

6. **Patient Authorizations Required:** If Vendors, Volunteers or Observers will have access to or contact with patients, either in person or remotely viewing patient care, an attending physician must obtain the patient’s permission for the visitor’s presence.
   a. The request for permission may be offered, and the agreement or objection received, verbally and documented in the patient’s health record.
   b. The patient may also sign an Authorization to Use or Disclose Protected Health Information. (See Forms)
   c. If the patient has signed an informed consent for surgery or other procedure that includes consent for observers, then no further written or verbal authorizations are required.

7. **Privacy Policies for Vendors:** Vendors or other company representatives who are demonstrating or supervising uses of their services or products within UF patient care areas must either register through the current vendor tracking system (RepTrax) or complete the following steps:
   a. Check in with the appropriate clinic or department, and
   b. If not completed within the past 12 months, complete the HIPAA for Visitors and Vendors training module, review the Health Information Policy, and sign UF’s Confidentiality Statement.
   c. A Health Science Center clinic or department representative must obtain written authorization from patient(s) for the vendor(s) to be present, as needed.
   d. Retain originals of all above vendor documentation in the designated college, department, or clinic administration office. Give a copy of all signed documents to the vendor.
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.1. Visitors, Vendors, Volunteers and Observers (continued)

8. Privacy Policies for Volunteers:
   a. Volunteers, whether volunteering for assigned duties or simply observing for periods longer than 21 consecutive days, may be registered for up to one year at a time; they must renew their application and registration annually, if applicable.
   b. Non-professional and non-licensed students and other individuals who want to volunteer to work in UF outpatient clinical care areas should apply through the Shands Volunteer Office; or apply through the Student Health Care Center to work in that facility.
   c. If needed for the performance of the duties assigned to them, Volunteers may have limited direct access to restricted data, including PHI, with written approval from the UF Privacy Office. Such access would only occur during authorized activities such as, for example, using paper-based health records or departmental databases for research or clerical duties. Access to the current electronic health record system using a personal logon and password is not included.
   d. Students, research scholars, and clinical professionals, both national and foreign, who want to volunteer (to work or to observe):
      1) In the College of Medicine: Contact the COM Dean’s Office – Administrative Services;
      2) In the colleges of Nursing, Public Health and Health Professions, Pharmacy, or Veterinary Medicine: Contact the Human Resources offices in those colleges;
      3) In the College of Dentistry: Contact the COD Clinic Administration Office;
      4) In the Student Health Care Center: Contact the SHCC Administration Office.
   e. Professional clinicians, therapists, and researchers who want to practice within their specialty as a volunteer must be appropriately licensed, credentialed, and registered with the sponsoring department.

9. Privacy Policies for Observing or “Shadowing”
   a. Observers may only be scheduled for up to three (3) consecutive weeks (21 continuous days) at a time. An observer desiring to stay longer may either apply to be re-registered for one subsequent visit (maximum of 21 days) or apply to register as a Volunteer. Each case will be considered individually.
   b. Observers must be accompanied and/or supervised by a UF healthcare representative at all times, and may not participate in patient care.
   c. Observers may, while being supervised in and as a result of their approved activities, view or hear limited amounts of restricted data, including PHI. No direct access to PHI is allowed.

B. DEFINITIONS

1. Observing or “Shadowing”: for the purposes of this policy and procedure, the extra-curricular viewing of patient care or health-related procedures that is outside the scope of a student’s required course work, or of a health care professional’s job duties; or viewing of patient care areas and/or health-related procedures by visitors (see definition following).
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.1. Visitors, Vendors, Volunteers and Observers (continued)

2. **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.

3. **Visiting**: for the purposes of this policy and procedure, time temporarily spent, to gain insight, knowledge, and experience, in a location that is not within the visitor’s normal scope of access or opportunity. The visitor is a guest, and not officially associated with the location by employment, contract, or any other formal written agreement.

4. **Volunteering**: providing, of an individual’s own free will, limited services that are within the scope of the individual’s expertise, with no monetary or material compensation for the services performed. Volunteers are not authorized to provide any direct patient care.

C. PRIVACY REQUIREMENTS

1. **Limited Access**: Access to PHI in any format must be limited to those persons who have a valid business or healthcare 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 from unauthorized access at all times, to protect the information from damage, loss, alteration, and tampering. (See also SECTION 5: Security of PHI: General Privacy Safeguards in this manual.)

D. PROCEDURES

1. **Sponsors** complete the following steps:
   a. Use the appropriate Request to Observe Patient Care form to register the Volunteer or Observer. Have the form approved by the Dean of the college where the volunteering or shadowing will occur and by the Privacy Office;
   b. Submit the completed Request to Observe Patient Care form and all attachments to the appropriate office as indicated at the bottom of the form.

2. **Volunteers**:
   a. **Volunteer forms** are available through UF’s Human Resources Services and through the college where the volunteer proposes to work. Volunteers make all arrangements with the assistance of the sponsoring department.
   b. **Complete UF’s training requirements**:
      1) Complete one online tutorial using an assigned UFID or a “dummy” number, as instructed, and print a certificate:
      a) HIPAA & Privacy – General Awareness, or
      b) HIPAA for Researchers: for volunteers involved in human research projects
6.1. Visitors, Vendors, Volunteers and Observers (continued)

2) Review the Health Information Policy and “sign” the UF Confidentiality Statement. (Registration in the electronic database is all that is required; actual signatures are not required.)

3. **Individual Observers:** Make arrangements to be sponsored by a representative working in one of UF’s health care components, and then complete the following steps prior to beginning activities at UF:
   a. Complete UF’s online training tutorial: HIPAA for Visitors & Vendors (use UF ID# 8888-####); print the certificate.
   b. Review the Health Information Policy and “sign” the UF Confidentiality Statement. (Registration in the electronic database is all that is required; actual signatures are not required.)

4. **Groups of Observers,** participating in scheduled teaching sessions that include either in-person or remote viewing of operative procedures or other patient care activities:
   a. The group’s UF sponsor completes a single Request to Observe Patient Care form for the group, following the procedure above, and submits it along with a Group Observation Roster listing all the proposed attendees.
   b. The attendees should:
      1) Complete the appropriate HIPAA training tutorial and sign the UF Confidentiality Statement.
      2) Sign the Group Observation Roster when they attend the session.
   c. After the observation, the sponsor should retain the completed Group Observation Roster with signatures along with a copy of the approved Request to Observe form. The sponsor should be prepared to produce the signed forms upon request, if audited for privacy compliance.

**E. REFERENCES:**

1. **HIPAA:** 45 CFR §164.501 (Definitions), §164.514(d) (Minimum Necessary Rule), §164.530 (Administrative Requirements), (b) (Training) and (e) (Sanctions)
2. **Florida Statutes:** 501.171 (Security of confidential personal information)
3. **University Rules:** UF-1.008 (Disruptive Behavior), UF-3.0031 (Volunteers), UF-3.046 and 3.047 (Disciplinary Procedures for Staff), UF-4.041 (Student Honor Code), and UF-7.048 (Disciplinary Actions for Faculty)
4. **UF Policies:** Information Technology (Acceptable Use Policy), Human Resources (Workplace Issues: Outside Employment Policy), Overview: UF DDD Memorandum 02/07/01 Outside Activities, Financial Interests and Conflict of Interest

**F. EXHIBITS**

1. Request to Observe Patient Care
2. Group Observation Roster
3. Volunteer Request to Observe or to Access Restricted Data

[Back to Table of Contents]
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.2. Student Data Access – Electronic Medical Records

A. POLICY

1. **Access to Medical Records**: Authorized University of Florida (UF) students will be provided with supervised access to protected health information (PHI), including personal account logins and passwords for the current electronic medical record (EMR) systems, based on the student’s program and curriculum needs.

2. **Pre-Approval Required for UF Students**: The UF Privacy Office must pre-approve all applications for access to the UF Health Information Systems for UF and UF-sponsored students who require such access to complete assigned academic course-work. The Privacy Office does not approve access applications for students from other colleges who do not have an academic relationship with UF. Students must be:
   a. Enrolled in a UF Health Science Center (HSC) College or a UF health-related program, or
   b. Pursuing an internship or clerkship rotation under an educational agreement with UF.

3. **Authorized Programs**: The following student groups have authorized access to the UF and Shands EMR as part of their academic requirements:
   a. **UF students in active clinical curricula**
      1) Medicine
      2) Physician Assistant
      3) Nursing
      4) Clinical Psychology
      5) Speech, Language and Hearing
      6) Communication Disorders / Hearing
      7) Pharmacy
      8) Dietetic
      9) Health & Human Performance
      10) Counseling Education
      11) Infection Control
      12) Visiting medical / health care students via Clinical Education Agreements with a UF HSC college
   b. **Special Programs**
      1) Junior Honors Medical Program – when necessary for research component
      2) MD PhD students – after completion of basic science curriculum

4. **Students Who Are Also Employees**: UF Students who are employed in jobs that require access to UF and Shands medical data for work-related purposes should not apply through the Privacy Office, but must apply directly through the UF and Shands Identity and Access Management (IAM) Department for such access, with the assistance of their employing department and approval by the employee’s supervisor.
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.2. Student Data Access – Electronic Medical Records (continued)

5. **Sponsor Responsibilities**: Students must be sponsored and supervised by a proctor or faculty member employed by one of UF’s Health Science Centers or the student’s UF health-related program.
   a. Sponsors provide the required information for each student at least three weeks, but not more than 60 days, prior to the access start date.
   b. Documentation created by students within paper or electronic health records must be co-signed by the student’s sponsor within 48 hours.
   c. The sponsor will be responsible for providing or obtaining written permissions for PHI uses when such permissions are required.
   d. The sponsor will periodically review students’ access rights to ensure they are only provided with the access needed to accomplish required academic tasks.
   e. The sponsor will immediately notify Information Services when a student’s enrollment status changes or is terminated.

6. **Time-Limits**: Student access is generally limited to 12 continuous months at a time, with start and end-dates defined at the time of application. Other procedures may be considered and/or arranged by the UF Privacy Office, in conjunction with the UF/SIAM Department, by special request.

7. **Access Standards**: Students are granted defined levels of access according to classifications established by UF and Shands IAM. The UF Privacy Office approves all role-based functions including reading, creating, and transporting health information.

8. **Shands Requirements**: Students must follow the Shands Information Systems requirements in addition to UF Privacy requirements when applying for access. Shands requirements include, but are not limited to:
   a. Signing the Shands Confidentiality and Security Agreement, which should be filed in the student’s record;
   b. Supplying necessary personal information for authentication purposes, and
   c. Participating in orientation training prior to using the Information Systems.

9. **Non-Compliance**: Immediate disciplinary action will be initiated by UF against students who misuse the UF Health Information System or the data maintained in the system. Violations may result in permanent loss of access privileges. Sanctions for misuse or misconduct will be recommended by the Privacy Office in collaboration with the student’s college.

10. **Use of Data**: Any data, including de-identified data, accessed by students may only be transported specific to class assignments, with advance written approval/direction of the student’s sponsor, and following Privacy Office policies for removal of patient data. (See **SECTION 2: Health Information Management: General Policies** in this manual.)
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.2. Student Data Access – Electronic Medical Records (continued)

11. **Research**: Students who are members of research teams, whether employed or working as volunteers, may use their currently approved EMR access for the research project as long as they are properly added to the IRB-approved protocol as an official member of the team, and the student continues in good, active, academic standing. Unauthorized student activities beyond the scope of the IRB-approved protocol can result in severe consequences for the Principal Investigator and the student.

   a. Unauthorized access to patient information will result in mandatory reporting to the Office for Civil Rights, as required by HIPAA/HITECH, and disciplinary action up to and including expulsion from UF.

   b. Students who are not actively associated with the programs listed above will not be provided personal access accounts to the EMR for research purposes. Patient information should be accessed through the Shands HIM department.

**B. DEFINITIONS**

1. **Protected Health Information**: Individually identifiable health information that is transmitted or maintained in any form or medium. (See full definition in Appendix A: Glossary)

2. **Personal Identification Information**: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual. (See full definition in Appendix A: Glossary)

3. **Transport**: To convey from one place to another; to remove from the premises.

**C. PRIVACY REQUIREMENTS**

Covered entities must do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity creates, receives, maintains, or transmits.

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.

d. Ensure compliance with the above by its workforce.

e. Implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process.

**D. PROCEDURES**

1. **Sponsors**

   a. **Complete the Access Application form** for any students who will need to use the system network, Apply at least two weeks, but not more than 60 days, in advance of the students’ arrival on campus.
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.2. Student Data Access – Electronic Medical Records (continued)

2) If there are more students than will fit on one page, use a second form, completing all the information at the top for each page; do not alter the form or write on the back of the form.

b. Provide the following information for each student:
   1) Sponsor’s name, title, and contact information;
   2) Student’s College, and specific Department, Division or Program;
   3) Student’s Name and UF Identification number;
   4) Student’s level or role: Graduate, Undergrad, Intern, etc.
   5) Date of the student’s expected graduation or departure
   6) Date on which SHC Confidentiality Statement was signed
   7) Access start and end dates:
      a) Access start date must be a future date;
      b) Access periods may not exceed 12 months, unless specifically pre-arranged.

c. Keep a copy of the Access Application form along with the students’ signed (Shands) Confidentiality Statements.

d. Forward the original Access Application form only to the Privacy Office, using the addresses provided at the bottom of the form.
   1) Do not send copies of the Shands Confidentiality Statements to the Privacy Office.
   2) Do not send Access Applications directly to Shands IAM unless specifically instructed to do so.

e. Pre-approval: The Privacy Office reviews and approves Access Applications prior to forwarding them to Shands IAM, usually within 24 hours. The Privacy Office may contact the sponsor for more information or if there are questions.

f. Notification: A notice that access has been granted, along with the corresponding logins and preliminary passwords will be sent to the sponsor by e-mail within 3-5 business days after applications have been submitted to the Privacy Office. If notice is not received within that time or if there is another problem, call the Privacy Office for assistance.

g. Changes: If dates of access need to be changed, submit a new form to the Privacy Office with the updated information and a note of explanation about the change.

h. Terminations: After access has been granted, if the access needs to be terminated prior to the requested End Date, call the Shands Help Desk; also send an e-mail to both the Shands IAM and the UF Privacy Office.

2. Students / Trainees

   a. Complete UF’s HIPAA & Privacy General Awareness Training and UF’s Confidentiality Statement. The successful completion and registration of these two components are automatically entered in a database and can be retrieved by your sponsor as needed.

   b. Sign a paper copy of the Shands Confidentiality Statement (available online) and fax, e-mail, or mail it to your sponsor.

   c. Complete the Shands online HIPAA training module after acquiring access to the system.
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.2. Student Data Access – Electronic Medical Records (continued)

d. **Renewal:** If you will need access to the HIS system for longer than 12 months, make a note of the date on which your current access will end, and remind your sponsor to submit a new Access Application before your access ends, so that your access will be uninterrupted.

e. **Other steps** may also be required by the student’s sponsor.

3. **UF Privacy Office:** review, sign, and forward approved Access Application forms to the Account Management Department of Shands IT.

4. **Shands IAM Department:** notify the Privacy Office and the Sponsor via e-mail when access has been granted, or contact the Privacy Office prior to granting access if there are problems or questions.

### E. REFERENCES

**HIPAA:** 45 CFR §164.306 Security standards: General rules, §164.308 Administrative safeguards

### F. EXHIBITS

1. **Form:** Student Data Access Application

2. **Matrix/Chart:** Student Data Access

[Back to Table of Contents]
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.3. Honest Broker System and Honest Broker Certification Process

A. POLICY: NEW: 06/01/2011

1. **Uses and Disclosures of PHI for Research:** The University of Florida (UF) will comply with privacy rule requirements of the Health Insurance Portability and Accountability Act (HIPAA) pertaining to the use and disclosure of protected health information (PHI) and de-identification of PHI used for research, as well as any applicable related state laws that are not preempted by HIPAA.

2. **Honest Broker Requirements:** An honest broker for research may be an individual, organization, or team certified to act for or on the behalf of a health-related tissue bank or databank to collect specified health information from the tissue or data bank, remove all patient identifiers, and provide the de-identified health information or tissue to research investigators in such a manner that it would not be reasonably possible for the investigators or other individuals to identify the patients directly or indirectly.

3. **Limited Data Sets:** If the health information provided to research investigators is based on a limited data set, as defined by HIPAA, the investigators must also complete and obtain Institutional Review Board (IRB) approval of a UF Data Use Agreement for Limited Data Sets. This Agreement addresses various HIPAA-mandated conditions related to subsequent uses and disclosures of limited data sets; it is reviewed and approved by the Privacy Office at the time of execution (see Limited Data Sets and Data Use Agreements in the HIPAA Privacy Management manual).

4. This policy applies to all UF entities and locations.

B. PRIVACY REQUIREMENTS

1. **Using De-Identified PHI:** PHI may only be used without patient authorization in a number of limited cases, one of which is where the PHI is de-identified. Prior written informed consent/authorization of patients for the research use of their de-identified existing health information is not required.

2. **De-Identification by Honest Brokers:** PHI can either be de-identified by an honest broker that is part of the covered entity (designated components as defined by UF) or by an honest broker which is a business associate of the covered entity. The honest broker cannot be one of the investigators or associated with the research team for which the honest broker performs duties.

3. **De-identified health information** must not include any of the eighteen identifiers defined by HIPAA, or any other identifiers, that would allow a reasonable possibility for the investigators or other individuals to identify the patients directly or indirectly.

4. **Re-Identification Codes:** The information provided to the investigators by the honest broker may incorporate linkage codes to permit information collation and/or subsequent inquiries (i.e., a “re-identification code”), however the information linking this re-identification code to the patient’s identity must be retained by the honest broker, secured and separate from research documents; all subsequent inquiries are conducted through the honest broker.
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.3. Honest Broker System and Honest Broker Certification Process (continued)

5. **Recruitment Aids:** This approach can also be used to identify eligible patients for subsequent recruitment into clinical trials by providing a de-identified listing of the health information of potential eligible subjects, including re-identification code numbers, to the clinical trial investigators.
   
a. The honest broker would subsequently provide the names of the identified patients to the patients’ personal physicians who would contact the patients to:
   1) Introduce the research study;
   2) Ascertain their interest in study participation; and
   3) Instruct the patients to contact the investigators or obtain their written authorization to share their interest in study participation with the investigators and to be contacted by them.

b. **Note that direct contact of the patients by the honest broker would constitute “cold-calling”, which is prohibited.**

**C. DEFINITIONS:**

1. **Honest Broker:** an individual, organization or team acting for, or on behalf of, the covered entity to collect health information, de-identify it, and provide it to research investigators in such a manner that it would not be reasonably possible for the investigators or others to identify the corresponding patients-subjects directly or indirectly.

2. **De-Identification:** Rendering PHI so that it is not individually identifiable. (See Appendix A: Glossary for full definition.)

3. **Limited Data Set:** A limited data set is PHI which excludes the previously listed direct identifiers of the individual, or of relatives, employers, or household members of the individual, except for:
   
a. Town or city, State, and zip code; and
   
b. Dates

**D. HONEST BROKER CERTIFICATION CRITERIA**

For an individual, organization or team to be an Honest Broker for UF, the proposed honest broker must be certified pursuant to the following process:

1. **Sponsorship or Appointment:** Honest Brokers must be independent of and unassociated with the research teams they work for.
   
a. Individual Applicants: must be sponsored by, but not employed by, a UF research investigator who:
      1) Is in good standing with a UF-recognized IRB of record, and
      2) Intends to use the honest broker’s services.
   
b. Organizations or Teams: The applicants must be:
      1) Appointed by a senior-level member of UF or Shands Administration
      2) Co-sponsored by the IRB Director
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.3. Honest Broker System and Honest Broker Certification Process (continued)

2. **Education and Training:** The proposed honest brokers must complete education and training, currently mandated by the IRB for all research investigators, prior to submitting an application. Links for this education and training may be found on the IRB-01 website under Education/Training (http://irb.ufl.edu/irb01/index.htm), and include:
   b. Completing the NIH Computer Based Training: **Protecting Human Research Participants**
   c. Completing UF’s **HIPAA for Researchers**.

3. **Application:** The individual or the organization or team must submit an application to become part of the UF- and IRB-certified Honest Broker System.
   a. The Honest Broker Certification applications are available at UF’s Privacy Office web site (http://privacy.health.ufl.edu).
   b. Applications should be submitted to the Honest Broker Coordinator in the UF Privacy Office: by the sponsoring investigator, for an individual; or by the Team Leader, for an organization or team.

4. **Attestation of Agreement:** All honest brokers must sign a written agreement that they will abide by all relevant UF and IRB guidelines, policies, and procedures, including continuing adherence to the UF honest broker certification criteria section of this policy, the duties and other requirements section (see Procedures, below), and the terms and conditions of the UF Business Associate Agreement for honest brokers (if applicable).

E. **PROCEDURES**

1. **Certification, Approval, and Maintenance**
   a. **Initial Review and Approval:** The UF Privacy Office will review and approve honest broker applications and related documentations are evaluated to determine that satisfactory evidence has been presented to meet or exceed the following certification criteria:
      1) Written documentation of the processes and/or systems to be used to develop both fully de-identified health information data sets and limited data sets, for both electronic and paper-based records;
      2) Written documentation of policies, procedures and controls necessary for:
         a) Compliance with the HIPAA Privacy Rule, the Federal Policy regulations for human subject protections (45 CFR 46) and UF’s Business Associate Agreement;
         b) Security and management of all PHI in the honest broker’s possession during the performance of honest broker functions;
         c) Audits and/or quality checks related to determining the efficacy of de-identification mechanisms;
         d) Security and management of re-identification keys; and
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.3. Honest Broker System and Honest Broker Certification Process (continued)

e) Maintenance and retention of work-product documentation for all work performed (for whom, what was provided, IRB approval info, etc.).

b. Ongoing Review and Maintenance: Each certified honest broker’s individual status will be reviewed at least annually by the Privacy Office. Changes in an honest broker’s status should be reported immediately by the sponsoring investigator or team leader.

2. Adding and/or Removing Brokers To/From a Service Team or Organization

a. Adding Brokers:

1) New brokers must first complete the education/certification modules as noted in the honest broker certification section above.

2) In accordance with UF policy, applicants who are not UF employees must complete and sign a business associate agreement (BAA).

3) A complete revision of the application must be submitted to the Privacy Office with any brokers to be added reflected in the revision. A copy of any relevant BAAs must accompany the revision documents. After the Privacy Office and the IRB approve the revision, a copy of the signed revised documents will be sent to the Team Leader of the service for distribution to members of the service.

b. Removing Brokers:

1) A complete revision of the application must be submitted to the Privacy Office with any brokers to be removed and the reason for the removal reflected in the revision.

2) After Privacy Office and the IRB approve the revision, a copy of the signed revised documents will be sent to the Team Leader of the service for distribution to members of the service.

3. Duties and Other Requirements of the Honest Broker: In order for a certified honest broker to work on behalf of investigators to de-identify PHI that is owned/held by UF, the honest broker must perform the following UF-defined duties and adhere to the following UF-defined requirements:

a. Non-UF honest brokers must execute a Business Associate Agreement with UF:

1) The terms of the BAA will specify continuing confidentiality requirements, duties and other expectations UF has of an honest broker service.

2) The generic UF Business Associate Agreement can be viewed at http://purchasing.ufl.edu. The generic Business Associate Agreement will be customized by UF to reflect the specific duties and other requirements UF specifies for honest broker services.

b. All certified honest brokers must ensure that approval of the IRB of record has been obtained for a research study before the honest broker acts on a request for de-identified PHI (from an investigator that is served by the IRB of record). This process may be as simple as being copied on an IRB approval letter from the IRB to the investigator. Likewise, the honest broker specified in a research application must have been prior-certified by the IRB of record in order for the IRB to approve the research application.
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.3. Honest Broker System and Honest Broker Certification Process (continued)

c. All certified honest brokers must adhere to any and all terms and conditions specified by the IRB of record for any research study for which the honest broker will perform de-identification services.

d. If an investigator requests a Limited Data Set, rather than a fully/completely de-identified data set:
   1) The IRB of record may require evidence of a completed Data Use Agreement for a Limited Data Set as part of its application process for approval of the proposed research involving the use of a Limited Data Set.
   2) An individual honest broker for the investigator must obtain (and retain) evidence of an appropriately executed Data Use Agreement in order to be granted access to the UF-held PHI.
   3) For organizations or Honest Broker Teams, a Data Use Agreement will provide necessary evidence, for audit purposes, of UF-required detailed disclosures (honest broker data set specifications) relative to:
      a) Where (in what UF entity) the PHI is located;
      b) What HIPAA-defined Limited Data Set elements are needed for the research;
      c) The purpose of the Limited Data Set request (detailed uses pertinent to the limited data set);
      d) Who (names, titles, addresses) will access, use and disclose the Limited Data Set information other than the principal investigator.

4. Honest Broker Data Requests: All requests for de-identified data must be documented. Elements to be recorded for each request include:

   a. Information from the investigator initiating the request:
      1) The Investigator’s name
      2) The date and time of the request entry
      3) The name of the study and the IRB approval number
      4) A detailed description of the needed data
      5) The requested turnaround time for the report
      6) Any special instructions

   b. Information from the honest broker handling the request:
      1) The name of the individual honest broker, whether working alone or as part of an organization or team
      2) The purpose of the request
      3) The data source(s) to be used
      4) The fields required to retrieve the data
      5) The method of output for the data
      6) Any special conditions, terms or instructions from the IRB

   c. Billing information, if the services provided will be compensated through an institutional account rather than through grant-funded mechanisms.
SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

6.3. Honest Broker System and Honest Broker Certification Process (continued)

d. Final disposition of the request:
   1) Date the data was retrieved
   2) Date the report was delivered
   3) Name of the honest broker delivering the report, if different from the one entering the request
   4) The name of the person to whom the data report was delivered

5. Non-Compliance

a. Failure by a UF-employed honest broker to abide by this policy will result in the suspension of the protocol while non-compliant actions are investigated. Non-compliance may result in disciplinary action for both the honest broker and the principal investigator pursuant to UF regulations and UF policy. Both employed and non-employee workforce members may also be sanctioned in accordance with applicable UF procedures.

b. Failure by any honest broker, including business associates, to abide by this policy may result in immediate termination of their UF certification to serve as an approved honest broker and immediate termination of their business associate agreement with UF.

c. Questions regarding this policy should be directed to the UF Privacy Office.

F. REFERENCES:

   HIPAA: 45 CFR Parts 160 & 164

G. EXHIBITS:

   Available on Request:
   1. Application for Honest Broker Certification (Individual)
   2. Application for Certification of Honest Broker Team/Process
   3. Attestation of Honest Broker Responsibilities
   4. Data Use Agreement

Back to Table of Contents