The HIPAA-specific policies in THIS MANUAL apply to all of the following: The University of Florida Health Science Centers, together including the UF Health Science Center clinics and physicians offices; the Florida Clinical Practice Association; the University of Florida Student Health Center, the University of Florida Speech and Hearing Clinic, the University of Florida Jacksonville Physicians, Inc.; the University of Florida Jacksonville Healthcare, Inc.; the University of Florida Colleges of Medicine, Nursing, Health Professions, Dentistry and Pharmacy; and other affiliated health care providers, including all employees, volunteers, staff and other University of Florida health services staff.

The Privacy Office
# Table of Contents

1. HIPAA: Federal Compliance Policies ........................................................................................................ 3  
2. HIPAA Organizational Requirements: Hybrid Entity ................................................................................ 6  
3. HIPAA Organizational Requirements: Organized Health Care Arrangement .......................................... 8  
4. HIPAA Organizational Requirements: Business Associates and Vendors ............................................... 10  
5. HIPAA: Policies, Procedures, and Document Maintenance ........................................................................ 14  
6. HIPAA: Responding to Requests for Restriction ...................................................................................... 16  
7. HIPAA: Responding to Requests for More Confidential Communications .............................................. 19  
8. HIPAA: Responding to a Request for Amendment of a Health Record .................................................. 22  
9. HIPAA: Responding to Opt-Out Requests for Fundraising ........................................................................ 26  
10. HIPAA: Responding to a Request for an Accounting of Disclosures ..................................................... 28  
11. HIPAA: Limited Data Sets and Data Use Agreements ............................................................................ 31  
12. HIPAA: Disclosures for Judicial and Administrative Proceedings ....................................................... 34  
13. HIPAA: Electronic Data Interchange - EDI .............................................................................................. 38  
15. HIPAA: Breach Notification for Privacy Violations .................................................................................. 48
1. **HIPAA: Federal Compliance Policies**

   **POLICY 03/28/2003**

   The University of Florida will endeavor to abide by the privacy and security rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as appropriate and as stated in the federal register.

   **DEFINITIONS**

   **Health Care Provider:** A provider of services (as defined in section 1861(u) of the Act, 42, USC1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 USC1395x(s)), and any other person organization who furnishes, bills, or is paid for health care in the normal course of business.

   **PRIVACY REQUIREMENTS**

   1. **Applicability:** It is understood that the standards, requirements, and implementation specifications adopted under the federally mandated Privacy Rules, commonly called HIPAA and discussed in this policy manual, apply to the University of Florida, which has defined itself as a Health Care Provider that maintains and transmits health information in electronic formats.

   2. **Preemption of State Law:** It is understood that a standard or requirement adopted under the privacy regulations that is contrary to a provision of State law will, in general, preempt the State law, except in certain limited situations, including:
      a. When a determination is made by the Secretary that the provision of State law is necessary:
      b. When the State law is more stringent in its provisions to protect the patient or provide the patient with greater rights. (See the Glossary for the definition of ‘more stringent’.)
      c. When the State law, including State procedures established under such law, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

   **NOTE:** The University of Florida has adopted the findings of the Florida State Law preemption analysis provided by the American Hospital Association.
1. **Principles for Achieving Compliance:** It is understood that the Secretary will seek the cooperation of covered entities, including the University of Florida, in obtaining compliance with the requirements of the privacy rules, and that the Secretary may provide technical assistance to covered entities to help them comply voluntarily with the requirements.

2. **Complaints to the Secretary:**
   a. It is understood that a person who believes The University of Florida is not complying with the requirements of the federal privacy regulations may file a complaint with the Secretary of Health and Human Services within 180 days of when the complainant knew or should have known that the act or omission occurred.
   b. It is also understood that the Secretary may investigate complaints and that the investigation may include a review of the pertinent policies, procedures, or practices of the University and of the circumstances regarding any alleged acts or omissions.

3. **Compliance Reviews:** It is understood that the Secretary may conduct compliance reviews to determine whether the University of Florida is complying with the applicable requirements of the privacy regulations.

4. **Responsibilities of Covered Entities:**
   a. It is understood that the University of Florida must keep records and submit compliance reports as prescribed by the Secretary to enable designated officials to ascertain whether the University is in compliance with the requirements of the privacy regulations.
   b. It is understood that the University of Florida must cooperate with investigations or compliance reviews conducted by the Secretary to determine whether it is complying with the requirements of the privacy regulations.

5. **Permit access to information:**
   a. It is understood that the University of Florida must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of the privacy regulations. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, the University must permit access by the Secretary at any time and without notice.
b. It is understood that protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable requirements of this part, or if otherwise required by law.

**RESOLUTION WHERE NONCOMPLIANCE IS INDICATED**

1. It is understood that, if an investigation or a compliance review indicates a failure to comply, the Secretary will so inform the University of Florida and, if the matter arose from a complaint, the complainant, in writing and attempt to resolve the matter by informal means whenever possible.

2. If the Secretary finds the University of Florida is not in compliance and determines that the matter cannot be resolved by informal means, the Secretary may issue to the University and, if the matter arose from a complaint, to the complainant, written findings documenting the non-compliance.

**RESOLUTION WHEN NO VIOLATION IS FOUND:**

It is understood that if, after an investigation or compliance review, the Secretary determines that further action is not warranted, the Secretary will so inform the University of Florida and, if the matter arose from a complaint, the complainant in writing.

**REFERENCES**

HIPAA Regulations: 45 CFR § 160.102 (Applicability), § 160.201 - 205 (Preemption), § 160.300 - 312 (Compliance)

**EXHIBITS: NONE**
2. **HIPAA Organizational Requirements: Hybrid Entity**

   **POLICY**

   1. The requirements of the federal privacy regulations apply only to the health care / medical components of the University of Florida.

   **DEFINITION**

   1. **Hybrid Entity:** The University of Florida has identified itself as a hybrid entity, according to the definition in the federal privacy regulations, as follows:
      a. The University is a single legal entity that is a covered entity;
      b. The University’s business activities include both covered and non-covered functions;
      c. The University is able to designate some of its components as medical components that are separate and distinct from non-medical components.

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

   **PRIVACY REQUIREMENTS**

   1. **Responsibilities:** The University of Florida, as a hybrid entity, has the following federally defined responsibilities.
      a. To comply with all federal compliance and enforcement requirements.
      b. To implement policies and procedures to ensure compliance with the safeguard requirements of the privacy regulations, including:
         1) The health care components do not disclose protected health information to other components in circumstances in which such disclosure would be prohibited if the components were separate and distinct legal entities;
         2) None of the components use or disclose protected health information in a way prohibited by law; and
         3) If a person performs duties for both a health care component and for another component as a member of the workforce, that person must not use or disclose protected health information in a way prohibited by law.
      c. To designate the components that are part of one or more health care components of the covered entity and to document the designation.
2. Identification of Medical and Non-Medical Components
   a. Medical Components of the University of Florida are listed in Chapter 1 of the UF Information Privacy Policies and Procedures: Health Information Operational Guidelines:  Relationship of University of Florida Components and Entities Explained
   b. Non-Medical Components are all other colleges and departments of the University of Florida.

REFERENCES

HIPAA Regulations: 45 CFR § 164.504 (Organizational Requirements)

EXHIBITS: NONE
3. **HIPAA Organizational Requirements: Organized Health Care Arrangement**

**POLICY**

<table>
<thead>
<tr>
<th>POLICY</th>
<th>REV: 06/01/2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Organization</strong>: The University of Florida and all its patient care areas have entered into an Organized Health Care Arrangement (OHCA) with the Shands HealthCare System; together they function as a seamless health care provider.</td>
<td></td>
</tr>
<tr>
<td>2. <strong>Joint Notice</strong>: For purposes of HIPAA compliance, the UF/Shands OHCA uses a Joint Notice of Privacy Practices and have agreed, as permitted by law, to share among themselves patient health information as needed for treatment, payment, and health care operations.</td>
<td></td>
</tr>
<tr>
<td>3. <strong>Separate Entities</strong>: These organizations are not in any way providing health care services mutually or on each other’s behalf. Shands HealthCare and the University of Florida are separate health care providers and each is individually responsible for its own activities, including compliance with privacy laws, and all health care services it provides.</td>
<td></td>
</tr>
</tbody>
</table>

**DEFINITION**

**Organized Health Care Arrangement (OHCA)**: An organized system of health care in which more than one covered entity participates, and in which the participating entities:

a. Hold themselves out to the public as participating in a joint arrangement; and
b. Participate in joint activities, including: Quality Assessment and Improvement activities and Payment activities.

**PRIVACY REQUIREMENTS**

1. A covered entity that participates in an organized health care arrangement (OHCA) may share protected health information about a patient with other covered entities that participate in the OHCA for any health care operations of the OHCA.

2. Covered entities that participate in an OHCA may present a Joint Notice of Privacy Practices (NPP), provided that all the participating covered entities agree to abide by the notice with respect to protected health information.

**PROCEDURES**

1. **Chief Privacy Officer**:

   a. Review and approve any proposals to participate in an Organized Health Care Arrangement prior to the University of Florida making an agreement with another covered entity.
b. Revise the Notice of Privacy Practices (NPP) as needed to document the participation of other covered entities or classes of covered entities in the OHCA.

c. Monitor the provision of the NPP by other members of the OHCA to assure that patients are, in fact, receiving the NPP as agreed.

d. Periodically monitor other joint activities of the OHCA.

2. **The Covered Entity:**

a. Share protected health information with the other OHCA participants, when such information is needed for treatment, payment, or health care operations, according to the provisions of the privacy regulations.

b. Provide the Joint NPP, if the entity is the first service provider.

**REFERENCES**

**HIPAA Regulations:** 45 CFR § 164.501 (Definitions), § 164.506 (Uses and Disclosures for Treatment, Payment, and Health Care Operations), § 164.520 (Notice of Privacy Practices)

**EXHIBITS:** NONE
4. **HIPAA Organizational Requirements: Business Associates and Vendors**

**POLICY**

1. **Permission to Disclose PHI:** Protected health information maintained by the University of Florida may only be disclosed to vendors and business associates (BA’s) who are contracted specifically to provide support services to the University. Business Associate Agreements (BAA’s) permit the disclosure of PHI to such contractors and holds the contractor accountable for safeguarding the PHI.

2. **Scope:** It is the responsibility of each department, division, or operating unit contracting for services with third parties where protected health information will be used or disclosed, to ensure that service agreements include the appropriate HIPAA-compliant verbiage, or that valid business associate agreements are executed.

3. **UF’s Responsibility:** The University of Florida is responsible if it becomes aware of a pattern of activity or practice of a contracted vendor or business associate that constitutes a material breach or violation of the business associate’s obligations. The University must take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful:
   a. Terminate the contract or arrangement, if feasible; or
   b. If termination is not feasible, report the problem to the Secretary.

4. **Business Associate’s Responsibility:** The HIPAA requirements that relate to privacy and security of protected health information and that are applicable to covered entities shall also be applicable to a business associate (including the business associate’s subcontractors) and shall be incorporated into the business associate agreement between the business associate and the covered entity. (HITECH Sec. 13401(a) and 13404(a))

**DEFINITIONS**

1. **Business Associate:** A person who, on behalf of a covered entity, performs, or assists in the performance of a function or activity or provides support services to the covered entity involving the creation, use, or disclosure of individually identifiable health information.

2. **Vendor:** A person who, on behalf of a covered entity, performs, or assists in the performance of a function or activity or provides support services to the covered entity. The activities may involve indirect or incidental exposure to individually identifiable health information.
PRIVACY REQUIREMENTS

1. The University is required to assure, to the extent practicable, that any business associate to whom it discloses PHI manages that information in compliance with federal and state privacy and security regulations.

2. Business Associate Contracts/Agreements: Business associate agreements must be in writing and must include terms authorized and approved by the University’s Privacy Office for maintaining compliance with federal privacy regulations.

3. Content of Contracts: Contracts between the University of Florida and business associates must:
   a. Clearly establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of the privacy regulations.
   b. Define the conditions to which the business associate will adhere, as follows:
      1) No use or further disclosure of the information other than as permitted or required by the contract or as required by law;
      2) Implementation of appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract, including:
         a) The BA must immediately report to the University any use or disclosure of the information not provided for by its contract of which it becomes aware.
         b) If the BA determines that personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person and that the information could be used for fraudulent purposes, the University must be notified immediately, if possible, but no later than 10 days after the determination is made.
         c) The BA must ensure that any agents, including subcontractors to whom it provides protected health information, agree to the same restrictions and conditions that apply to the business associate with respect to such information;
      3) Making available protected health information to patients, as required under rights of access and inspection, including:
a) Making available protected health information for amendment by the patient, and incorporating any approved amendments into protected health information maintained by the business associate;

b) Making available the information required to provide an accounting of disclosures;

c) A business associate included on a list provided by the University under Sec. 13405 (c)(3)(B) of the HITECH Act shall provide an accounting of disclosures (as required under paragraph (1) for a covered entity) made by the business associate upon a request made by an individual directly to the business associate for such an accounting.

4) Making available its internal practices, books, and records, concerning the use and disclosure of protected health information, to the Secretary for purposes of determining the University’s compliance with the privacy regulations; and

5) At termination of the contract, if feasible, return or destruction of all protected health information that the business associate still maintains in any form, retaining no copies of such information or, if return or destruction is not feasible, extending the protections of the contract to the retained information and limiting further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

6) Required implementation of administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic protected health information that it creates, receives, maintains or transmits on behalf of the covered entity;

7) Ensuring that any agent, including a subcontractor, to whom the business associate provides protected health information, agrees to implement reasonable and appropriate safeguards to protect it.

c. Authorize termination of the contract by the University of Florida, if at any time the University determines that a business associate has violated a material term or obligation under the agreement relating to HIPAA compliance.

1) The department that is party to the agreement and/or the University Chief Privacy Officer shall be notified and shall seek to immediately remedy the breach or, if that is not possible, to alter or terminate the agreement.

2) The University may also report violations to the Secretary of the Department of Health and Human Services.
4. **Purchase Orders:** Purchases with certain accounting codes (see Appendix C in this manual) have been identified as potential opportunities for exposing PHI. Where no contract exists, but HIPAA-related implications may apply for a general purchase, the Purchase Order will include the following statement, in lieu of a contract:

> VENDOR acknowledges that VENDOR may have access to protected health information (PHI) in various formats. VENDOR agrees to comply with all laws and policies covering security and confidentiality of PHI and to cooperate with the University of Florida’s monitoring of such compliance. VENDOR shall ensure that it will maintain all PHI in a secure and confidential fashion and that no PHI is disclosed to any third party except as permitted by law. VENDOR shall not disclose any PHI without first obtaining consent from the person to whom the record pertains or that person’s legal representative.

**PROCEDURES**

1. Identify the type of client for which the Business Associate Agreement (BAA) is to be written:
   a. Refer all clinical Business Associate Agreements to the Health Science Center Office of Contracts and Related Services.
   b. Refer all other non-clinical Business Associate Agreements to the UF Purchasing Office.

2. Provide the contract office or the purchasing office with the information necessary to complete the appropriate Business Associate Agreement template, including all required privacy and security safeguards.

3. When BAA template language is materially changed, the Privacy Office must approve the changes. Legal review of a changed agreement may also be required.

**REFERENCES**

1. **HIPAA Regulations:** 45CFR §160.103 (Definitions), §165.504 (Organizational Requirements)

2. **HITECH Act:** Sec. 13401 and 13404 (Application of Privacy Provisions and Penalties to Business Associates), Sec. 13405 (c) (Accounting for Certain Disclosures...)

3. **Florida Statute:** 817.568 and 817.5681 (Criminal Use of Personal Identification Information)

**EXHIBITS:**

- Appendix C: Accounting Codes for Purchase Orders
5. **HIPAA: Policies, Procedures, and Document Maintenance**

<table>
<thead>
<tr>
<th>POLICY:</th>
<th>REV: 11/01/2006</th>
</tr>
</thead>
</table>

1. **Development:** The University of Florida has developed policies and procedures with respect to protected health information that comply with federal and state regulations. The Chief Privacy Officer is responsible for developing, maintaining and revising all privacy policies and procedures.

2. **Revisions:** The University of Florida will revise policies and procedures as needed to maintain compliance with changes in the law. Policies and procedures are also reviewed at least annually, and revised as needed.

3. **Notice of Changes:** Any changes in privacy practices or in privacy policies and procedures are documented and published on the Privacy Office web site as soon as possible; reasonable efforts are made to communicate the changes to individuals who may be affected by them. The revision date of policies and procedures appears on each document.

4. **Right to Change:** The University of Florida reserves the right to change its policies and procedures at any time, and to make such changes effective for protected health information that it has created or received prior to the effective date of the revision.

5. **Availability:** Policies and procedures are maintained by the Privacy Office in written form, which may be printed and/or electronic formats. Copies are available on the University of Florida Privacy Office web site. Paper copies may be obtained from the Privacy Office during normal business hours.

6. **Maintenance:** Any communication, action, activity, or designation that is required by federal or state privacy regulations to be documented or in writing (i.e., training records, complaint investigations, privacy audits, accounting logs, etc.) will be maintained by the responsible college, department, or unit in writing, (which may be printed and/or electronic formats) for at least six years from the date of creation or the last effective date, whichever is later.

**DEFINITIONS**

1. **Policy:** An overall plan defining goals and objectives.

2. **Procedure:** A series of steps or processes used to achieve stated goals; a set of formalized instructions.

3. **Documentation:** Evidence or substantiation that certain actions were completed, information was collected, used or disclosed, or requirements were met.
PRIVACY REQUIREMENTS

The following policies and procedures will be maintained to comply with federal and state privacy laws and regulations:

1. Identification of Medical and Non-Medical Components
2. Maintaining Confidentiality of Health Information
3. Reporting, Investigating and Responding to Privacy Violations
4. Health Information and Record Management
5. Designated Record Set
6. Retention, Archiving and Disposal of Private Information
7. Patient’s Rights Regarding Health Information
8. Uses and Disclosures of Protected Health Information
9. Privacy and Research
10. Security Safeguards
11. Training for Privacy and Security

REFERENCES

HIPAA Regulations: 45 CFR §164.530(i) & (j) and §164.316(a) & (b) (Policies and Procedures and Documentation)

EXHIBITS: NONE
6. **HIPAA: Responding to Requests for Restriction**

<table>
<thead>
<tr>
<th>POLICY</th>
<th>REV.: 06/01/2010</th>
</tr>
</thead>
</table>

1. **Right to Request Restrictions:**
   a. Patients and personal representatives are permitted to request restrictions of uses and disclosures of protected health information normally available for treatment, payment, or health care operations. The University of Florida is not obligated to agree to these requests, but will review all requests and respond to the patient in writing within a reasonable period of time.

   b. The University must comply with a patient or representative’s request to restrict certain protected health information under the following conditions:
      1) 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,
      2) 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.

2. **Authority:** Only the Chief Privacy Officer may agree to requests for restrictions, after consultation with appropriate personnel representing the patient care area affected by the request. Requests that are agreed to by any other personnel will not be valid.

3. **Response:** If the University of Florida agrees to any request for restriction, it must adhere to the terms of the agreement until the agreement is terminated, either by the patient or the University. The designated management representative must ensure that all the records to which restrictions apply are appropriately flagged.

**DEFINITIONS**

**Restriction:** A specifically defined limitation of use or disclosure of an element of protected health information 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.

**PRIVACY REQUIREMENTS**

1. **Patients have the right** to request that the University of Florida restrict uses or disclosures of protected health information about the patient to carry out treatment, payment or health care operations.

2. **The University is not required to agree** to a request for 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 protected health information 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. If a restriction is agreed to, the University must not use or disclose the restricted information, except in cases where the patient is in need of emergency treatment and the information is essential to the treatment.

4. The University may terminate its agreement to a restriction if:
   a. The patient agrees to or requests the termination in writing;
   b. The patient orally agrees to the termination and the oral agreement is documented.
   c. The University informs the patient that it is terminating its agreement, and that the termination only affects information created or received after notifying the patient.

**PROCEDURES**

1. The Privacy Office:
   a. Review the completed Requests for Special Privacy Protections forms to verify the scope of the requested restriction and to determine if the University of Florida is capable of effectively and consistently restricting the use or disclosure, as requested.
   b. Discuss the requested restriction with all patient care areas affected by the request, as needed.
   c. Document the decision to grant or deny the restriction on the Response to Request for Special Privacy Protections form.
   d. File the original Response form in the Privacy Office along with the original Request form.
   e. Send a copy of the Response to the requestor, or delegate this duty to a clinic manager or supervisor. Send a copy of the Response to the appropriate area to be filed in the patient’s health record.
   f. Restrictions agreed to by the University should be reviewed if the Privacy Office is notified of any difficulties in abiding by the restriction, or of any problems that arise as a result of the restriction.

2. Patient Care Areas: 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 the process established for such a restriction.
3. **Document the termination of a restriction** on a Termination of Special Privacy Protections form. File the original Termination form with the original Request and Response forms in the Privacy Office.
   a. Send a copy of the Termination form to the patient.
   b. Send a copy of the Termination of Special Privacy Protection form to the appropriate area to be filed in the patient’s health record.
   c. Notify all patient care areas affected by the termination.

4. **A new Request for Special Privacy Protections** should be completed for any additional restriction requests and should follow the same procedure outlined above. (Each request makes all previous requests obsolete. The new form should contain all restrictions requested - not just the most recent request.)

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

**REFERENCES**

**HIPAA Regulations:** 45 CFR § 164.501 (Definitions); § 164.522 (Right to Request Privacy Protections)

**HITECH Act:** Sec. 13405(a) (Restrictions on Certain Disclosures)

**EXHIBITS**

**Form:** Response to Request for Special Privacy Protections

**Form:** Termination of Special Privacy Restrictions
7. **HIPAA: Responding to Requests for More Confidential Communications**

<table>
<thead>
<tr>
<th>POLICY</th>
<th>03/28/2003</th>
</tr>
</thead>
</table>

1. **Permitted to Request:** Patients and personal representatives are permitted to request to receive written communications (reports, bills, etc.) in an alternative manner or location. Such requests should be in writing and addressed to the Privacy Office.

2. **Response:** The University of Florida is not obligated to agree to these requests, but will review all requests and respond to the patient in writing within a reasonable period of time.
   a. Requests of this type do not include routine changes of address, but refer to requests requiring special arrangements outside the normal course of business.
   b. The University of Florida will accommodate or deny the patient’s request based on:
      1) The ability of the University of Florida to consistently accommodate the request,
      2) Whether the patient can specify an alternative location or method of contact, and
      3) The potential impact of the change on the University’s routine health care operations.

3. **Authority:** Only the Privacy Office, in consultation with appropriate personnel representing the patient care area affected by such a request, may agree to requests for more confidential written communications. Requests that are agreed to by any other personnel will not be valid.

4. **Terms:** If the University of Florida agrees to any alternative communication method, it must adhere to the terms of the agreement until the agreement is terminated, either by the patient or the University.
   a. The designated management representative must ensure that all the records to which such agreements apply are appropriately flagged.
   b. Communication methods or locations agreed to by the University should be reviewed if the Privacy Office is notified of problems that arise as a result of the agreement.

**DEFINITIONS**

1. **Verbal Communications:** Includes face-to-face 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.
PRIVACY REQUIREMENTS

1. The University of Florida must permit patients to request, and must accommodate reasonable requests, to receive communications of protected health information from the University by alternative means or at alternative locations.

2. The University of Florida may not require an explanation from the patient as to the basis for the request as a condition of providing the confidential communications.

PROCEDURES

1. **Review the completed Request form** with the supervisor or Manager of the patient care area(s) affected.
   a. Verify the alternative manner or location for communications,
   b. Determine if the request is reasonable, and
   c. Determine if the University of Florida is able to effectively and consistently accommodate the request.

2. **Document the decision** to grant or deny the request on a Response to Request for Special Privacy Protections form. File the original Response form in the Privacy Office along with the original Request form.
   a. Send a copy of the Response to the requestor, or delegate this duty to a clinic manager or supervisor.
   b. Send a copy of the Response to the appropriate area to be filed in the patient’s health record.

3. **Document a change or the termination** of a communication agreement on a Termination of Special Privacy Protections form. File the original Termination form with the original Request and Response forms in the Privacy Office.
   a. Send a copy of the Termination form to the patient.
   b. Send a copy of the Termination of Special Privacy Protection form to the appropriate area to be filed in the patient’s health record.
   c. Notify the managers or administrators of all patient care areas affected by the termination.

4. **Retain all documentation** for a period of at least six years after the date that it was last in effect.

REFERENCES
HIPAA Regulations: 45 CFR § 164.501 (Definitions); § 164.522 (Right to Request Privacy Protections)

**EXHIBITS:**

**Form:** Response to Request for Special Privacy Protections

**Form:** Termination of Special Privacy Restrictions
8. **HIPAA: Responding to a Request for Amendment of a Health Record**

<table>
<thead>
<tr>
<th>POLICY</th>
<th>REV: 06/01/2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Permitted to Request:</strong> Patients and personal representatives are permitted to request an amendment or correction of a health record, if they feel it is inaccurate or incomplete.</td>
<td></td>
</tr>
<tr>
<td>2. <strong>The University of Florida is not obligated to agree</strong> to these requests, but will review all requests and respond to the patient in writing within a reasonable period of time.</td>
<td></td>
</tr>
<tr>
<td>a. <strong>NOTE:</strong> Requests of this type do not include routine changes of address or other demographic information, but refer to extraordinary or disputed additions or corrections to a record that require special arrangements outside the normal course of business.</td>
<td></td>
</tr>
<tr>
<td>3. <strong>The Chief Privacy Officer may designate representatives</strong> to receive and process patients’ requests for amendments.</td>
<td></td>
</tr>
<tr>
<td>4. <strong>Response:</strong> 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. The University may reasonably limit the length of a statement of disagreement from the patient.</td>
<td></td>
</tr>
</tbody>
</table>

### DEFINITIONS

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

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

### PRIVACY REQUIREMENTS

1. The University has the right to require that requests for correction or amendment be submitted in writing and that the request includes a reason to support the requested amendment.

2. The University of Florida must act on the patient’s request for a correction or amendment no later than 60 days after receipt of such a request.

3. The University of Florida may deny a patient’s request for correction or amendment, if it determines that the protected health information or record:
a. Was not created by the University of Florida, unless the patient provides reasonable evidence that the originator of the PHI in question is no longer available to act on the request;
b. Is not part of the University of Florida designated record set;
c. Would not be available for inspection under the right to access; or
d. Is accurate and complete.

**PROCEDURES**

1. **Review the completed request** with a representative from the clinic or department, or with the author of the original documentation, to determine if the amendment is warranted.

2. **Document the grant or denial** of the request by completing the lower portion of the Request for Amendment form.
   a. If the request is denied, document the reason(s) for the denial on a Response to Request for Amendment form, and notify the patient or representative. Notification of a denial of a request must contain:
      1) The basis for the denial.
      2) A notification of the individual’s right to submit a written statement disagreeing with the denial and procedures for filing such a statement.
      3) A statement that if a statement of disagreement is not submitted, the individual may request that the facility provide the individual’s Request for Amendment and the University’s Denial of Request with any future disclosure of the protected health information that is the subject of the amendment.
      4) A description of how the individual may file a complaint with the University of Florida Privacy Office or the Secretary of Health and Human Services pursuant to HIPAA regulations.
   b. If the request cannot be completed for some reason, document the reason(s) for the delay on a Response to Request for Amendment form only. Do not complete the lower portion of the Request for Amendment form.
   c. File all original forms in the Privacy Office. Send copies of documentation to the appropriate areas to be filed in the patient’s record. Send copies of the Request for Amendment and the Response forms to the patient.

3. **If the correction / amendment is determined to be warranted:**
   a. For corrections of original material,
1) Notify the author of the original material, if available, that the entry may be corrected, using approved error-correction procedures.

2) If the author of the material is no longer available, an entry may be made by, and at the discretion of, the patient’s current practitioner to clarify or amend the incorrect information. No entry may be removed or destroyed.

3) If the correction is warranted and is part of a transcribed report, a note will be added to the electronic report to indicate that a correction has been made. Contact the Shands HI/RM Transcription supervisor to obtain the procedure for noting corrections in dictated reports.

b. For amendments (adding new material to the health record), notify a supervisor or other designated person to add the amendment to or near the part of the designated record set that is affected or provide a link (by whatever method is most appropriate) to the location of the amendment.

c. Make reasonable efforts to inform and provide the correction / amendment to persons identified by the patient as needing the new material.

4. If the request for amendment is denied, and the patient chooses to submit a written statement disagreeing with the denial, file the statement with the original Request and Response forms. Send a copy of the statement to the appropriate area to be filed in the patient’s health record.

5. Prepare a written rebuttal, if necessary and appropriate, to the patient’s statement of disagreement and file it with the patient’s statement of disagreement. Send a copy of the rebuttal to the patient who submitted the statement of disagreement; also have a copy of the rebuttal filed in the patient’s health record.

6. Append or otherwise link the patient’s request for an amendment, the University’s denial of the request, the patient’s statement of disagreement, if any, and the University’s rebuttal, if any, to the designated record set.

7. Future disclosures:
   a. The patient’s request for amendment and its denial, or an accurate summary of such information, must be included with any subsequent disclosure of the protected health information, only if the patient has requested such action.
   b. All statements of disagreement and rebuttals must be included, or, at the election of the University, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.
8. **If another provider informs** the University of Florida of an amendment to a patient’s protected health information, notify the appropriate patient care area(s) to amend the protected health information in the designated record sets it possesses.

9. **All documentation** concerning the request for correction or amendment should be maintained in the Privacy Office for at least six years. Copies of the request documentation should be placed in the patient’s health record.

**REFERENCES**

**HIPAA Regulations:** 45 CFR § 164.501 (Definitions); § 164.526 (Right to Request an Amendment)

**EXHIBITS:**

**Form:** Response to Request for Amendment
9. **HIPAA: Responding to Opt-Out Requests for Fundraising**

<table>
<thead>
<tr>
<th>POLICY</th>
<th>REV: 06/01/2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Opt-Out:</strong> Patients are permitted to either confirm their acceptance of, or “opt-out” of, receiving fundraising solicitations and materials. The University will take appropriate measures to ensure that individuals who request to opt out of receiving future fundraising communications are not sent such communications.</td>
<td></td>
</tr>
<tr>
<td>2. <strong>Annual Attestation Statement:</strong> Entities involved in fundraising for the University’s healthcare components must sign a statement annually attesting to compliance with HIPAA regulations.</td>
<td></td>
</tr>
</tbody>
</table>

**DEFINITIONS**

1. **Fundraising:** To solicit and acquire monetary and other resources for an institution or organization

2. **Opt-Out:** To express a desire to no longer participate in a given activity; express instruction by a customer, or a recipient of a mail, email, or other direct delivery to stop the sender from sending information or more messages.

**PRIVACY REQUIREMENTS**

1. **Patients are informed** in the Notice of Privacy Practices:
   a. That the University is permitted to use limited health information for fundraising purposes, and
   b. How the patient may “opt-out” of receiving fundraising communications.

2. **The University is required** to make reasonable efforts to ensure that individuals who opt out of receiving future fundraising communications are not sent such communications.

**PROCEDURES**

1. **Include the following elements** in all fundraising materials sent to patients by the University of Florida:
   a. A description of how the patient, by completing and signing an authorization, may give permission for the University to:
      1) Continue to send fundraising communications i.e., (to affirm in writing their wish to be included in future solicitations); and
      2) Use or disclose the patient’s protected health information for the purpose of fundraising.
b. A description of how the patient may “opt out” of receiving further such communications (i.e., to affirm in writing their wish to be excluded from further solicitations).

2. **Add the patient’s name** and identification information to the “Opt Out” log maintained in the Privacy Office.

3. **Forward the patient’s request** and information to the University of Florida Foundation, the Shands Privacy Office, and other fundraising entities of the HSC, as appropriate.

4. **Maintain the patient’s original request** in the Privacy Office for at least six years after it was last in effect, or the patient’s final episode of care, whichever is later.

5. **The fundraising entity** will provide and maintain Authorizations to Use or Disclose PHI for Fundraising, Marketing, or Public Relations (see Forms) from those persons who have specifically agreed to receive fundraising communications.

6. **If the University discloses PHI** while engaging in fund-raising on behalf of another entity, it must track such disclosures of PHI for disclosure accounting purposes. (See Accounting for Disclosures in this manual.)

**REFERENCES**

**HIPAA Regulations:** 45 CFR § 164.501 (Definitions); § 164.514(f)(1) (Other Requirements)

**HITECH Act:** Sec. 13406(b) (Opt Out of Fundraising)

**EXHIBITS: NONE**
10. **HIPAA: Responding to a Request for an Accounting of Disclosures**

<table>
<thead>
<tr>
<th>POLICY</th>
<th>REV: 06/01/2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Patient’s Rights:</strong> Patients have the right to receive an accounting of PHI disclosures made from the patient’s health record with certain exceptions. See Privacy Requirements below.</td>
<td></td>
</tr>
<tr>
<td>2. <strong>Response:</strong> The University of Florida must act on the patient’s request for an accounting no later than 60 days after receipt of such a request.</td>
<td></td>
</tr>
<tr>
<td>3. <strong>System Requirements:</strong></td>
<td></td>
</tr>
<tr>
<td>a. UF’s web-based Disclosure Tracking System must be used to record all appropriate disclosures, which occur outside of UF’s electronic health record systems, and will be used to assist in compiling an accounting of disclosures when requested.</td>
<td></td>
</tr>
<tr>
<td>b. UF’s electronic health records systems must include the capability of tracking uses and disclosures of protected health information for treatment, payment, and health care operations purposes, as well as for other authorized and unauthorized purposes.</td>
<td></td>
</tr>
<tr>
<td>4. <strong>Retention:</strong> The web-based Disclosure Tracking System entries must be maintained for at least six years from the date of the individual disclosures. Disclosures tracked through an electronic health record system, must be maintained for at least three years.</td>
<td></td>
</tr>
</tbody>
</table>

**DEFINITION**

1. **Disclosure:** The release, transfer, provision of access to, or divulging in any manner, of protected health information held by the University of Florida to an entity or person outside the University.

2. **Use:** The sharing, employment, application, utilization, examination, or analysis of individually identifiable information within an entity that maintains such information.

**PRIVACY REQUIREMENTS**

1. **Information to be included** in each accounting of disclosures includes:
   a. The date of the disclosure;
   b. A brief description of the PHI disclosed;
   c. The name and address of the entity or person who received the PHI, if known; and
   d. The purpose of the disclosure.
2. **Exceptions:** The University is **not** required to account for the following types of disclosures:
   a. **Disclosures made from a paper record system** to carry out treatment, payment and health care operations *(NOTE: The HITECH Act removes this exception for uses and disclosures made “through an electronic health record”)*;
   b. To patients, when requesting PHI about themselves;
   c. Incidental to a use or disclosure otherwise permitted or required;
   d. Pursuant to a valid authorization by the patient;
   e. For the facility’s patient directory;
   f. To persons directly involved in the patient’s care;
   g. For national security or intelligence purposes;
   h. To correctional institutions or law enforcement officials that have custody of a patient;
   i. Disclosures that occurred prior to April 14, 2003.

3. **Process:** In response to a request from an individual for an accounting, the University may elect to provide either:
   a. An accounting of disclosures of protected health information that were made by the University and by a [specific] business associate acting on behalf of UF; or
   b. An accounting of disclosures that were made only by the University, and provide a list of all business associates acting on behalf of UF, including contact information for such associates (such as mailing address, phone, and email address).

**PROCEDURES: PRIVACY OFFICE**

1. **Requests for accountings** of disclosures should be received in writing, and should be accompanied by a photocopy of the patient’s paper or electronic Disclosure Log, if one exists, from the clinical area that initially received the request.
   a. If the request involves health records held by Shands HIM Department, forward a copy of the letter to that department.
   b. If the request is the second or subsequent request within a 12-month period, inform the patient or representative of the fees for compiling the accounting before beginning.

2. **Sources:** Refer to any paper disclosure logs from the patient’s record, then to the web-based database (Disclosure Tracking System), and finally, to the electronic tracking...
system within the appropriate electronic health record system. Account only for disclosures made during the time period specified in the request.

a. Accounting for disclosures for research: Notify all Principle Investigators of the request and need to respond within 10 working days.

b. Accounting for disclosures to and by business associates: Any business associates involved with the patient’s care or payment should be notified and requested to account for any qualifying disclosures within 10 working days.

3. **Multiple disclosures:** If the University of Florida has made multiple disclosures of PHI to the same person or entity for a single purpose, provide:
   a. The required information (see above) for the first disclosure during the accounting period;
   b. The frequency and/or number of the disclosures made during the accounting period; and
   c. The date of the last such disclosure during the accounting period.

4. **For second and subsequent requests** within a 12-month period, calculate fees for the accounting at an hourly rate; include all persons involved in compiling the requested information, up to but not exceeding $50.00 total.

5. **Compile the information** from all sources and enclose it in a letter to the patient. Retain the original request (and copy of the disclosure log) in the Privacy Office along with a copy of the letter sent to the patient.

6. **Send a copy** of the letter to the appropriate area to be filed in the patient’s health record.

**REFERENCES:**

HIPAA Regulations: 45 CFR § 164.520 (Notice of Privacy Practices), § 164.528 (Accounting of Disclosures)

HITECH Act: 13405(c) (Accounting of Certain PHI Disclosures...)

**EXHIBITS: NONE**
11. **HIPAA: Limited Data Sets and Data Use Agreements**

<table>
<thead>
<tr>
<th>POLICY</th>
<th>REV: 07/01/2010</th>
</tr>
</thead>
</table>

1. **The University of Florida is permitted** by law to use or disclose a limited data set only for the purposes of research, public health, or health care operations.

2. **Use of limited data sets** is strictly controlled and must be approved before a person or entity within the University of Florida enters into any agreements. After approval, a limited data set may be used or disclosed, only if a data use agreement is established with a recipient.
   a. A limited data set created by the university may include a link field to allow re-identification of the individual. The link field may incorporate portions of direct identifiers; for example, initials plus a sequence number or an encrypted portion of a SSN.
   b. The limited data set is subject to the minimum necessary rules of HIPAA.
   c. The limited data set is not subject to disclosure accounting.
   d. Whenever a limited data set is to be used or disclosed for research, public health, or health care operations purposes, the university requires the use of the Data Use Agreement template. The limited uses and disclosures of the protected health information will be defined in detail by the purpose statements in the data use agreement.

3. **For Limited Data Sets as they relate to the Minimum Necessary Rule**, see the policy and procedure entitled “Minimum Necessary Rule” in the Operational Guidelines.

4. **Creating a Limited Data Set:**
   a. If an outside entity creates a limited data set on behalf of the University of Florida, using protected health information received from UF, it must have first signed a business associate agreement with UF.
   b. If a University of Florida employee creates the limited data set, that employee, will, for that purpose, be a member of the UF HSC workforce, and shall complete appropriate HIPAA training and follow applicable UF policies regarding privacy of health information.
DEFINITIONS

1. **Limited Data Set**: A limited data set is protected health information that excludes the following direct identifiers of the patient or of relatives, employers, or household members of the patient:
   a. Names;
   b. Postal address information, other than town or city, State, and zip code;
   c. Telephone numbers;
   d. Fax numbers;
   e. Electronic mail addresses;
   f. Social security numbers;
   g. Health record numbers;
   h. Health plan beneficiary numbers;
   i. Account numbers;
   j. Certificate/license numbers;
   k. Vehicle identifiers and serial numbers, including license plate numbers;
   l. Device identifiers and serial numbers;
   m. Web Universal Resource Locators (URLs);
   n. Internet Protocol (IP) address numbers;
   o. Biometric identifiers, including finger and voice prints; and
   p. Full face photographic images and any comparable images.

2. **Data Use Agreement**: An agreement or contract that establishes the uses and disclosures of protected health information by the recipient of a limited data set.

PRIVACY REQUIREMENTS

1. **Data Use Agreement Required**: The University of Florida may use or disclose a limited data set only if a data use agreement is established stating that the recipient will only use or disclose the protected health information for limited purposes.

2. **Contents**. A Data Use Agreement must:
   a. Establish the permitted uses and disclosures of such information by the recipient. The Data Use Agreement may not authorize the recipient to use or further disclose the information in a manner that would violate federal privacy regulations;
   b. Establish and define who is permitted to use or receive the Limited Data Set; and
   c. Provide that the Limited Data Set recipient will:
1) Not use or further disclose the information other than as permitted by the agreement or as otherwise required by law;
2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the agreement;
3) Report to the covered entity any use or disclosure of the information not provided for by its Data Use Agreement of which it becomes aware;
4) Ensure that any agents, including subcontractors, to whom it provides the Limited Data Set agree to the same restrictions and conditions that apply to the recipient; and
5) Not identify the information or contact the patients.

3. **Compliance:** The University of Florida is required, if a pattern of activity or practice of a Limited Data Set recipient were discovered, that constituted a material breach or violation of the Data Use Agreement, to take immediate reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:
   a. Discontinue disclosure of protected health information to the recipient; and
   b. Report the problem to the Secretary of Health and Human Services.

**PROCEDURE**

Contact the UF Department of Sponsored Research or the UF HSC Office of Contracts and Related Services to apply for a Data Use Agreement. Do not attempt to compose or initiate a Data Use Agreement without authorization.

**REFERENCES**

HIPAA Regulations: § 164.514 (e) (Limited Data Sets)

**EXHIBITS:** NONE
12. HIPAA: Disclosures for Judicial and Administrative Proceedings

**POLICY**

1. **Permitted Disclosures:** The University of Florida may disclose protected health information (PHI) in the course of any judicial or administrative proceeding in response to:
   a. An order of a court or administrative tribunal, in which the University will only disclose the PHI expressly authorized by such order; or
   b. A lawfully issued subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:
      1) The University receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to notify the patient who is the subject of the protected health information of the request; or
      2) The University receives satisfactory assurance from the party seeking the information that a qualified protective order has been secured.

2. **Notice to the Patient:** The University of Florida may disclose PHI in response to any lawful process described above without receiving satisfactory assurance if the University itself makes reasonable efforts to provide notice to the patient or to seek a qualified protective order.

3. **Super-Confidential Health Information** maintained by the University of Florida that is subject to specific state or federal laws (mental health, STD, HIV, etc.) will only be disclosed in accordance with those laws.

4. **Review:** All disclosures of PHI in response to court orders are reviewed by a qualified health record professional who is specifically trained to manage requests for PHI.

**DEFINITIONS**

1. **Lawfully Issued Subpoena** means 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. **Satisfactory Assurance** (for the purposes of Policy paragraph 1.b.1) above) means receipt of a written statement and accompanying documentation demonstrating that:
   a. The party requesting information has made a good faith attempt to provide written notice to the patient (or, if the patient’s location is unknown, to mail a notice to the patient’s last known address);
b. The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the patient to raise an objection to the court or administrative tribunal; and

c. The time for the patient to raise objections to the court or administrative tribunal has elapsed, and:
   1) No objections were filed; or
   2) All objections filed by the patient have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

3. **Satisfactory Assurance** (for the purposes of Policy paragraph 1.b.2) above) means receipt of a written statement and accompanying documentation demonstrating that:
   a. The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
   b. The party seeking the protected health information has secured a qualified protective order from such court or administrative tribunal.

4. **Qualified Protective Order** (for purposes of Policy paragraph 1.b.2) above) means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
   a. Prohibits the parties from using or disclosing the protected health information 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 protected health information (including all copies made) at the end of the litigation or proceeding.

---

**PRIVACY REQUIREMENTS**

The provisions of this section do not supersede other provisions of the federal privacy regulations or other state laws that otherwise permit or restrict uses or disclosures of protected health information.

---

**PRIVACY OFFICE PROCEDURES:**

1. **Review all subpoenas and court orders requesting health information** that have been forwarded from clinics or departments where no record copying services are employed, using the following guidelines:
UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
HIPAA PRIVACY MANAGEMENT

a. Subpoena from an attorney representing the patient, requesting health information concerning the patient:
   1) Must be accompanied by a valid authorization to disclose Protected Health Information, signed by the patient or the patient’s representative.
   2) If no authorization is attached, contact the requesting attorney to request one. Provide a copy of the University’s Authorization form, if necessary.

b. Subpoena issued by a Florida court from an attorney representing another party (i.e. insurance company, physician, hospital, etc.) requesting health information concerning a patient:
   1) Must be accompanied by one of the following documents before records may be released:
      a) A certificate of compliance from the attorney that contains all of the requirements under HIPAA (see attached example);
      b) A valid authorization to disclose Protected Health Information signed by the patient or the patient’s personal representative; or
      c) A court order for the release of the patient’s information
   2) If none of the documents is attached, contact the requesting attorney or send an appropriately worded copy of the sample letter to the attorney to request an authorization, a certificate, or a court order.

c. Subpoenas issued by other state courts from an attorney representing another party (i.e. insurance company, physician, hospital, etc.) requesting health information concerning a patient:
   1) Do not honor subpoenas from other states unless they are “lawfully issued” through a court in the State of Florida. (See Definitions)
   2) Send the appropriately worded sample letter to the requesting attorney stating that the subpoena must be issued by or under the jurisdiction of a Florida court.

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

2. If approved, notify the clinic or department to proceed with processing the subpoena or court order in accordance with the required timelines.

3. If the judicial order is not approvable, notify the clinic or department and explain the issues or deficiencies. If necessary, assist the record custodian in contacting the requestor for clarification or more documentation.
REFERENCES

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

EXHIBITS

Certificate of Compliance
HIPAA: Electronic Data Interchange - EDI

POLICY

Voluntary Compliance: The University of Florida will comply with all applicable parts of the federal Privacy Rule relating to electronic data interchange (EDI).

DEFINITIONS

1. Code Set means any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes.

2. Data Set means a semantically meaningful unit of information exchanged between two parties to a transaction.

3. Electronic Data Interchange: Electronic transfer of information, such as electronic media health claims, in a standard format between trading partners.

4. National Provider Identifier (NPI): The standard unique health identifier for health care providers; a 10-position numeric identifier, with a check digit in the 10th position, and no intelligence about the health care provider in the number.

5. Standard Transaction: A transaction that complies with the applicable standard adopted under this part. Standard transactions include:
   a. Health care claims or equivalent encounter information
   b. Payment and remittance advice
   c. Claim status inquiry and response
   d. Eligibility inquiry and response
   e. Referral certification and authorization inquiry and response
   f. Enrollment and disenrollment in a health plan
   g. Health plan premium payments
   h. Coordination of benefits

6. Trading partner agreement: An agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement.

PRIVACY REQUIREMENTS

1. General Rule. If the University of Florida conducts with another covered entity (or within the same covered entity), using electronic media, a transaction for which the
Secretary has adopted a standard, the transaction must be conducted as a standard transaction (see definition above).

2. **Exception for direct data entry transactions.** A health care provider electing to use direct data entry offered by a health plan to conduct a transaction for which a standard has been adopted must use the applicable data content and data condition requirements of the standard when conducting the transaction. The health care provider is not required to use the format requirements of the standard.

3. **Use of a Business Associate.** The University of Florida may use a business associate, including a health care clearinghouse, to conduct a transaction covered by the EDI standards. If UF chooses to use a business associate to conduct all or part of a transaction on its behalf, the university must require the business associate to:
   a. Comply with all applicable requirements of the EDI regulations.
   b. Require any agent or subcontractor of the business associate to comply with all applicable requirements of the privacy and security regulations.

4. **Trading Partner Agreements.** The University may not enter into a trading partner agreement that would:
   a. Change the definition, data condition, or use of a data element or segment in a standard.
   b. Add any data elements or segments to the maximum defined data set.
   c. Use any code or data elements that are either marked “not used”, or are not in, the standard’s implementation specification(s).
   d. Change the meaning or intent of the standard’s implementation specification(s).

5. **National Provider Identifiers.** The University of Florida, as a covered healthcare provider, must:
   a. Obtain an NPI from the National Provider System (NPS) for itself and for any subparts that would be a covered health care provider if it were a separate legal entity.
   b. Use the NPI to identify itself on all standard transactions that it conducts where its health care provider identifier is required.
   c. Disclose its NPI, when requested, to any entity that needs to identify the University as a covered health care provider in a standard transaction.

6. **Code Sets - General requirements.** When conducting a standard transaction as described above, the University must meet the following requirements:
a. Medical data code sets: Use the applicable medical data code sets described in §162.1002 that are valid at the time the health care is furnished.

b. Nonmedical data code sets: Use the nonmedical data code sets as described in the implementation specifications that are valid at the time the transaction is initiated.

**PRIVACY OFFICE PROCEDURES**

None

**REFERENCE:**

**HIPAA:** CR Part 162.100 - 1902: Electronic Data Interchange

**EXHIBITS:** NONE

<table>
<thead>
<tr>
<th>POLICY</th>
<th>REV: 06/01/2010</th>
</tr>
</thead>
</table>
| The University of Florida will implement and maintain appropriate safeguards to comply with the specifications of the federally mandated Security Rule, which require covered entities to protect the confidentiality and integrity, and to maintain the availability of all electronic protected health information (PHI) created, received, maintained, or transmitted by the University and affiliated entities. These safeguards include:
| c. Protection against reasonably anticipated threats or hazards to the security or integrity of such information.
| d. Protection against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
| e. Mandatory compliance with the federal Security Rule and Florida State laws by all members of the workforce of healthcare components of the University of Florida and affiliated entities. |

**DEFINITIONS**

1. **Administrative safeguards**: administrative actions, policies, and procedures, implemented to manage the security measures and the conduct of workforce members for the protection of PHI.
2. **Authentication**: the corroboration that a person is the one claimed.
3. **Availability**: making data or information accessible and useable upon demand.
4. **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.
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. **Malicious software**: software, for example, a virus, designed to damage or disrupt a system.
8. **Password**: confidential authentication information composed of a string of characters.
9. **Physical safeguards**: physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.

10. **Security incident**: the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

11. **Technical safeguards**: the technology and the policy and procedures for its use that protect electronic PHI and control access to it.

12. **User**: a person or entity with authorized access.

13. **Workstation**: an electronic computing device or any other device that performs similar functions and electronic media stored in its immediate environment.

**HIPAA SECURITY REQUIREMENTS**

1. **Implementation**: A covered entity is required to use security measures that allow it to reasonably and appropriately implement the standards and implementation specifications as specified in the Security Rule.

2. **Administrative Safeguards** to be implemented:
   a. **Appointment of a Security official**: This individual is responsible for the development, implementation, and enforcement of the policies and procedures required by the Security Rule.
   b. **Written policies and procedures**:
      1) To prevent, detect, contain, and correct security violations.
      2) For authorizing access to electronic PHI, for ensuring that all members of the workforce have appropriate access to electronic PHI, and for preventing unauthorized workforce members from obtaining access to electronic PHI.
      3) To investigate security incidents, and recommend appropriate disciplinary action, sanctions, and mitigation.
      4) For responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic PHI.
   c. **Training**: A security awareness and training program for all members of its workforce (including management).
   d. **Evaluations**: A schedule of periodic evaluations to measure an entity’s compliance with the requirements of the Security Rule.
3. **Physical Safeguards** to be implemented:
   
a. **Written policies and procedures:**
   
   1) To limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
   
   2) That specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI.
   
   3) That govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility.
   
b. **Physical protections** for all workstations that access electronic PHI, to restrict access to authorized users.

4. **Technical Safeguards** to be implemented:
   
a. **Authentication Procedures:** to verify that a person or entity seeking access to electronic PHI is the one claimed.
   
b. **Written policies and procedures:**
   
   1) To allow access only to those persons or software programs that have access rights for electronic systems that maintain PHI.
   
   2) To protect electronic PHI from improper alteration or destruction.
   
c. **Hardware, software, and/or procedural mechanisms** that record and examine activity in information systems that contain or use electronic PHI.
   
d. **Security measures** to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.

---

**PRIVACY OFFICE PROCEDURES**

1. **Implementing Administrative Safeguards**
   
a. Preventing, Detecting, Containing, and Correcting Security Violations When electronic PHI is Involved
   
   1) **Risk analysis (Required).** Assist with conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the University.
2) **Risk management (Required).** Assist with the implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

3) **Sanction policy (Required).** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity when electronic PHI is involved.

4) **Information system activity review (Required).** Implement procedures to regularly review records of electronic PHI information system activity, such as audit logs, access reports, and security incident tracking reports.

b. **Authorizing Access to Electronic PHI**

1) **Authorization and/or supervision (Addressable).** Monitor the authorization of defined access and supervision of workforce members who work with electronic PHI or in locations where it might be accessed.

2) **Workforce clearance procedure (Addressable).** Determine that the access of a workforce member to electronic PHI is appropriate.

3) **Termination procedures (Addressable).** Monitor terminations of access to electronic PHI when the employment of a workforce member ends or as otherwise required.

c. **Security Awareness and Training Program**

1) **Security reminders (Addressable).** Assist with publishing and otherwise communicating periodic security updates involving electronic PHI.

2) **Protection from malicious software (Addressable).** Assist with the establishment of procedures for guarding against, detecting, and reporting malicious software.

3) **Log-in monitoring (Addressable).** Assist with monitoring log-in attempts and responding to discrepancies, as requested.

4) **Password management (Addressable).** Assist with establishing and communicating procedures for creating, changing, and safeguarding passwords.

d. **Responding to Security Incidents when electronic PHI is involved**

1) Identify and respond to suspected or known security incidents involving electronic PHI;

2) Mitigate, to the extent practicable, harmful effects of such identified security incidents; and

3) Document the privacy related issues associated with such security incidents and their outcomes.
e. Contingency Plans for Emergencies

1) **Data backup plan (Required).** Assist with the creation and maintenance of retrievable exact copies of electronic protected health information, as necessary.

2) **Disaster recovery plan (Required).** Assist with restoration of any loss of restricted data.

3) **Emergency mode operation plan (Required).** Monitor and assist with continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.

4) **Testing and revision procedures (Addressable).** Review period testing and assist with revisions of contingency plans, as needed.

5) **Applications and data criticality analysis (Addressable).** Work with IT Security to assess the relative criticality of specific applications and data in support of other contingency plan components, as needed.

g. **Evaluation of Security Rule Compliance:** Work with IT Security to perform periodic technical and nontechnical evaluations that establish the extent to which the University’s security policies and procedures meet the requirements of the Security Rule.

2. **Implementing Physical Safeguards**

a. Limiting Physical Access to Electronic Information Systems

1) **Contingency operations (Addressable).** Assist with defining contingency routes for facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

2) **Facility security plan (Addressable).** Assist with establishing and maintaining safeguards for the facility and the equipment therein from unauthorized physical access, tampering, and theft.

3) **Access control and validation procedures (Addressable).** Assist with controlling and validating each person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

4) **Maintenance records (Addressable).** Review and monitor documented repairs and modifications to the physical components of a facility that are related to security of electronic PHI (for example, hardware, walls, doors, and locks).

b. Workstations
1) **Accountability (Addressable).** Monitor the maintenance of records of the movements of hardware and electronic media and any person responsible for them, as needed.

2) **Device and media controls.** Assist with monitoring and controlling the movement of hardware and electronic media that contain PHI into and out of a facility, and within the facility.

3) **Disposal of Electronic PHI (Required).** Implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored.

4) **Media re-use (Required).** Assist as needed with the removal of electronic PHI from electronic media before the media are made available for re-use.

5) **Data backup and storage (Addressable).** Assist with and monitor the creation of a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.

3. **Implementing Technical Safeguards**
   a. **Controlling Access**
      1) **Unique user identification (Required).** Assist in assigning a unique name and/or number for identifying and tracking user identity, as needed.
      2) **Emergency access procedure (Required).** Assist to establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.
      3) **Automatic logoff (Addressable).** Establish policies and monitor compliance with processes to terminate an electronic session after a predetermined time of inactivity.
      4) **Encryption and decryption (Addressable).** Establish policies and facilitate the implementation of a mechanism to encrypt and decrypt electronic protected health information.

   b. **Auditing Activity**
      1) **Hardware, software, and/or procedural mechanisms.** Periodically audit activity in information systems that contain or use electronic PHI.
      2) **Integrity.** Establish policies and procedures to protect electronic PHI from improper alteration or destruction, and monitor activities as needed.
      3) **Mechanism to authenticate electronic PHI (Addressable).** Periodically audit electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.
c. Authentication: Monitor and assess verification procedures, which establish that a person or entity seeking access to electronic protected health information is the one claimed.

d. Transmission Security

1) Integrity controls (Addressable). Establish policies and facilitate the implementation of security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.

2) Encryption (Addressable). Establish policies and facilitate the implementation of a mechanism to encrypt electronic PHI whenever deemed appropriate.

REFERENCE:

HIPAA: 45 CFR § 164.302 – 164.316 (Security Standards)

Florida Statutes: 817.568 & 817.5681 (Criminal use of personal information)

EXHIBITS:

None
15. **HIPAA: Breach Notification for Privacy Violations**

<table>
<thead>
<tr>
<th>POLICY</th>
<th>REV: 06/01/2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.</td>
<td></td>
</tr>
</tbody>
</table>

**DEFINITIONS**

1. **Breach:** the unauthorized acquisition, access, use, or disclosure of protected health information, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

   *Exceptions.*—The term “breach” does not include—

   (i) Any unintentional acquisition, access, or use, or disclosure of protected health information by an employee or individual acting under the authority of a covered entity or business associate if—

   (I) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; **and**

   (II) such information is not further acquired, accessed, used, or disclosed by any person; **or**

   (ii) Any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; **and**

   (iii) Any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

2. **Unsecured Protected Health Information:** 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.
3. **Personal Identification Information:** Any data that may be used, alone or in conjunction with any other information, to identify a specific individual, including, but not limited to: name, postal or electronic mail address, telephone number, social security number, date of birth, mother’s maiden name, driver’s license number, passport number, credit or debit card number, unique biometric data (fingerprint, voice print, retinal image), medical records, etc.

4. **Privacy Complaint:** An allegation by an individual that an organization is not complying with the requirements of the federal privacy and/or security regulations or the organization’s own policies and procedures related to the privacy / security of personal information.

5. **Privacy Incident:** A known or suspected action, inconsistent with the organization’s privacy policies and procedures, or an adverse event, related to protected health information.

6. **Notification:** The act of informing persons affected by a breach of private information that their information was included and steps they can take to protect themselves and their privacy.

### PRIVACY REQUIREMENTS

1. **Individual Notice:** Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information.

   a. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.

   1) If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside.

   2) If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

   b. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach.

   c. Notifications must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps
affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity.

d. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

2. Media Notice: Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction.

a. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area.

b. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

3. Notice to the Secretary In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form.

a. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.

b. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis.

c. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

4. Notification by a Business Associate: If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach.

a. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach.

b. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any
PROCEDURES:

The Privacy Office will initiate its Breach Response Procedure upon notification of a breach of PHI which meets the description of this policy.

REFERENCES

1. HIPAA Regulations: 45 CFR § 160.306 (Complaints to the Secretary), § 164.400 – 414 (Breach Notification) and § 164.530(d) (Complaints), (e) (Sanctions), and (f) (Mitigation)
2. University Rules: Rules 6C1-1.008(1)(o), 6C1-3.047(3)(d), 6C1-4.016(2)(o) and (t), and 6C1-7.048(1)(c)
4. Florida Statutes: 817.568 & 817.5681 (Criminal use of personal information)

EXHIBITS:

None