Section 1: GENERAL PRIVACY RULES

1.6 Reporting and Responding to Violations involving Protected Health Information

POLICY

1. **Expectations:** The University of Florida (UF) promotes 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.

   The University of Florida (UF) Privacy Office will review and investigate all privacy-related complaints and reported incidents of information privacy or security, as needed.

2. **Reporting:** All unauthorized acquisition, access, use, or disclosure 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.

3. **Reviewing Complaints:** All complaints and reported violations of information privacy and security will be investigated according to Privacy Policy 1.7 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. **Confidentiality:** All investigations and resulting documentation of privacy-related complaints and incidents are strictly confidential and shall not be disclosed to anyone unrelated to an alleged or confirmed violation, unless required by law.

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

6. **Investigations and Disciplinary Action:** Privacy Office staff are 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.

   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.

7. **Personnel:** Privacy analysts appointed by, and under the supervision of, the UF Privacy Office will review and determine action on privacy complaints and incidents reported to the UF Privacy Office.

8. 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.
    a. The following factors will be evaluated to determine the best mitigation strategies:
        - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
        - The unauthorized person who used the PHI or to whom the disclosure was made;
        - Whether the PHI was actually acquired or viewed; and
        - 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.
9. Required Notification for Breaches of PHI and/or Other Restricted Data:
    c. 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.
    d. The 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.
    e. 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 Legal Affairs of any breaches of security, as required by and using the terms as defined by the Florida Statutes.
10. Documentation: Investigations, interviews, and determinations regarding privacy-related complaints and incidents will be documented and the documentation will be maintained for at least six (6) years, or longer, if required by law or other circumstances.

DEFINITIONS

1. *Investigation:* A formal or systematic examination or research of a privacy complaint or incident.
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. *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.
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 policies and procedures, or an adverse event, related to restricted data or PHI.
6. *Security Incident:* the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

7. *Unsecured Protected Health Information:* 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); specifically, encryption for electronic PHI, and destruction for all other PHI.

PRIVACY REQUIREMENTS

1. Policies and Procedures: A covered entity (CE) 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.
2. Notification: A CE 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 CE to have been, accessed, acquired, used, or disclosed as a result of such breach.
3. Mitigation: A CE must mitigate, to the extent practicable, any harmful effect that is known to the CE of an access, acquisition, use or disclosure of PHI in violation of its policies and procedures or the requirements of the Privacy Rule by the CE or its business associate.
4. Sanctions: A CE must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the CE or the requirements of the Privacy Rule. A CE or business associate must apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the CE or business associate.
5. Disclosures by whistleblowers: A CE is not considered to have violated the HIPAA requirements if a member of its workforce or a business associate discloses PHI, provided that:
    a. The workforce member or business associate believes in good faith that the CE has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the CE potentially endangers one or more patients, workers, or the public; and
    b. The disclosure is to:
        i. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the CE 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 CE; or
        ii. 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.
6. Refraining from intimidating or retaliatory acts: A CE 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:
        i. Filing of a complaint with the Secretary under the HIPAA regulations;
        ii. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under the HIPAA regulations; or 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.

WORKFORCE REQUIREMENTS

1. Preventing Privacy Incidents:

a. Take reasonable precautions to avoid incidental disclosures:

i. Speak in a low, soft voice while discussing private information;

ii. Move to as private a location as possible while using private information;

iii. 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:

i. Know and follow UF's policies and procedures concerning proper handling of PHI.

ii. 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.

iii. 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:

a. If an unauthorized (accidental or intentional) acquisition, access, use, or disclosure of PHI or restricted data occurs, or is suspected to have occurred:

i. 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.

ii. If the breach involves a computer system containing private data:

- Take immediate steps to secure the affected system. Follow UF and departmental information security procedures.
- 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).
- 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 Personal Identification Information (not PHI).

b. Include the following information when reporting an Incident:

   i. Date, time and location of the incident;

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

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

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

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

   vi. 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?

   vii. 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.

   viii. 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.

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

   i. 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.

   ii. For All UF-Jacksonville HSC colleges, departments and clinics, UF Health Proton Therapy Institute, and all UFJPI Clinics: report to the UF-Jacksonville Privacy Manager.

5. Additional Procedures for Managers

a. Responding to Loss or Inappropriate Disclosure of Information

   i. Misplaced or Stolen Paper Records:

   - 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.
   - 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.

   ii. Inappropriate Disclosures: If PHI or other restricted data is e-mailed, mailed, faxed, or otherwise delivered to an incorrect address or the wrong individual:

   - Report all instances of misdirected information on an Incident Report to the Privacy Office as soon as they are discovered.
   - It is better to wait for instructions from the Privacy Office before notifying the affected patient.
   - If the recipient reports the erroneous delivery, document the conversation and/or include any written communications from the recipient with the Incident Report.

- 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.
- Document these efforts and the results on the Incident Report form.
- Document any verbal assurances from the recipient that the information was destroyed or deleted.
- Log the disclosure into the online Disclosure Tracking System, if instructed to do so.

REFERENCES

1. Florida Statutes: 112.3187, Florida's Whistle-blower's Act; 817.568, Criminal use of personal information; 501.171, Security of confidential personal information
2. HIPAA Regulations: 45 CFR §160.306 Complaints to the Secretary, 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;

EXHIBITS

1. Incident and Complaint Forms: Incident Report – Protected Health Information
2. Incident and Complaint Forms: Privacy Complaint
3. Recommended Sanctions for Violations of Privacy by Faculty and Staff (Appendix A)
4. Recommended Sanctions for Violations of Privacy by Students (Appendix B)

Appendix A: Recommended Sanctions for Violations of Privacy by Faculty and Staff 08/15/2007

Level of Violation	Cause or Motivation	Type of Violation	Examples of Violations	Recommended Actions
Level I Errors in handling Restricted Data, or in maintaining workstation security measures.	Unintentional Lack of training Inexperience Poor judgment Poor process	• Clerical Error • Process Error • Technical Error • Judgment Error	• Leaving an active computer screen with access to PII unattended. • Leaving PII, in any format, unattended in public areas. • Disclosing PII without identity verification. • Sending PII to wrong postal or e-mail address • Placing non-shredded documents in inappropriate waste receptacles	• Retraining and/or re-evaluation. • Specialized training and evaluation. • Discussion of policy and procedures. • Verbal warning or oral reprimand. • New Confidentiality Statement signed
Level II Breach in the terms of the Confidentiality Statement and/or UF policies concerning use and disclosure of Restricted Data.	Intentional, but non-malicious Curiosity Concern Compassion Carelessness Compulsiveness	• Un-authorized • Non-job- related • Stealth	• Failure to complete required Privacy Training, and/or to sign the UF Confidentiality Statement. • Discussing PII in public or other inappropriate areas. • Accessing the record of any person, including co-workers, friends, or family, without professional Need-to-Know • Using someone else's computer account. • Copying information as a favor • Installing unauthorized software with potential to harm systems. • Adding, deleting, or altering electronic information	• Letter of Reprimand, requiring written corrective action in response. • Suspension of information system privileges • Suspension of employment
Level III Breach in the terms of the Confidentiality Statement and/or UF Policies concerning use and disclosure of Restricted Data, for personal gain or to affect harm on another person.	Malicious intent Financial gain Revenge Protest Gross Negligence	• Theft, including Identity theft • Malicious actions: i.e., o alteration or deletion of data, o making data or systems inaccessible	• Access and unauthorized disclosure of PII for personal gain or to affect harm on another person. • Unauthorized access of celebrity or VIP PII for any reason. • Malicious alteration, deletion or removal of PII, from UF facilities. • Unauthorized publication or broadcasting of PII. • Repeated Level I or II violations	• Final written warning and/or • Termination of information system user privileges • Revocation of Medical Staff privileges • Termination of employment.

Appendix B: Recommended Sanctions for Violations of Privacy by Students 08/15/2007

Level of Violation	Cause or Motivation	Type of Violation	Examples of Violations	Recommended Actions
Level I Errors in handling Restricted Data, or in maintaining workstation security measures.	Unintentional Lack of training Inexperience Poor judgment Poor process	• Clerical Error • Process Error • Technical Error • Judgment Error	• Leaving an active computer screen with access to PII unattended. • Leaving PII, in any format, unattended in public areas. • Disclosing PII without identity verification. • Sending PII to wrong postal or e-mail address • Placing non-shredded documents in inappropriate waste receptacles	• Retraining and re-evaluation. • Specialized training and evaluation. • Discussion of policy and procedures. • Verbal warning or oral reprimand. • New Confidentiality Statement signed
Level II Breach in the terms of the Confidentiality Statement and/or UF policies concerning use and disclosure of Restricted Data.	Intentional, but non-malicious Curiosity Concern Compassion Carelessness Compulsiveness	• Un-authorized • Non-job- related • Stealth	• Failure to complete required Privacy Training, and/or to sign the UF Confidentiality Statement. • Discussing PII in public or other inappropriate areas. • Accessing the record of any person, including co- workers, friends, or family, without professional Need- to-Know • Using someone else's computer account. • Copying information as a favor • Installing unauthorized software with potential to harm systems. • Adding, deleting, or altering electronic information without authorization.	• Letter of Reprimand, with written corrective action plan. • Loss of University privileges, including use of University library, parking, computers, and athletic / entertainment functions. • Conduct Suspension
Level III Breach in the terms of the Confidentiality Statement and/or UF Policies concerning use and disclosure of Restricted Data, for personal gain or to affect harm on another person.	Malicious intent Financial gain Revenge Protest Gross Negligence	• Theft, including Identity theft • Malicious actions: i.e., o alteration or deletion of data, o making data or systems inaccessible	• Access and unauthorized disclosure of PII for personal gain or to affect harm on another person. • Unauthorized access of celebrity or VIP PII for any reason. • Malicious alteration, deletion or removal of PII, from UF facilities. • Unauthorized publication or broadcasting of PII. • Repeated Level I or II violations	• Expulsion or suspension.