

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
HEALTH INFORMATION OPERATIONAL GUIDELINES

I. Reporting and Responding to Privacy Violations

A. POLICY

Rev. 11/01/2006

1. **Expectations:** The University of Florida promotes ethical standards of conduct and encourages all members of its workforce and the workforce of its affiliated entities to honor the privacy rights of patients, clients, students, employees, and volunteers.
2. **Unauthorized disclosures** or acquisitions of private data, known and suspected, must be reported to the UF Privacy Office immediately.
3. **All complaints and reported violations** of information privacy and security will be investigated. If violations of privacy are confirmed, the University will recommend corrective actions and sanctions, and will try to mitigate, to the extent possible, any harmful effect of a confirmed privacy violation.
4. **The University will make reasonable efforts to notify** affected persons if it is determined that their personal identification information (PII) was, or is reasonably believed to have been, acquired by an unauthorized person and that the information could be used for fraudulent purposes.
 - a) *The UF-Gainesville Privacy Office will oversee all aspects of the notification process,*
 - b) *The College, Department, Division, Clinic, or other University unit from which the information was acquired will be responsible for the costs and labor associated with notifying the affected persons.*

B. DEFINITIONS

1. **Accidental Disclosures:** Unintentional disclosures that occur as a result of circumstances beyond the control of the individual, even though established policies and procedures were followed. Accidental disclosures are considered Privacy Incidents.
2. **Incidental Disclosures:** Unintentional disclosures during the normal course of business, which are incidental to an otherwise permitted use or disclosure of the information. If a workforce member is taking reasonable precautions, and another individual happens to see or overhear private data that the workforce member is using, the workforce member will not be held liable for that disclosure and usually does not need to report it as an incident.
3. **Intentional Disclosures:** Disclosures of private data that occur as a result of careless or deliberate and/or pre-meditated disregard of established policies and procedures, with or without malicious intent. Intentional disclosures are Privacy Incidents and will result in disciplinary action and the application of sanctions by the University. They may also result in personal liability, either in civil or criminal legal action.
4. **Mitigation:** To make less severe, to partially remove, or to correct, so that harmful effects of a privacy violation are reduced or eliminated.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
HEALTH INFORMATION OPERATIONAL GUIDELINES

5. **Privacy:** Freedom of an individual from intrusion or observation; the right to maintain sole control over personal information; and the expectation that others will respect the individual's rights.
6. **Professional Need to Know:** Specific and limited information necessary to complete assigned work.
7. **Restricted Data:** Any and all personal identification information, financial information, protected health information, and other information protected by law (i.e., student records and reports; or, human resource data, including disciplinary actions).
8. **Security:** Administrative, physical and technical safeguards, used to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration or destruction, and to maintain the integrity of the information.
9. **Security Incident:** The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
10. **Violation:** Infraction of a law; going against established rules.

C. PRIVACY REQUIREMENTS

1. **Reporting Privacy Violations:** All UF workforce members, who are employed by or otherwise associated with the University of Florida's healthcare components and affiliated entities, are obligated to report any known or suspected violations, breaches or unauthorized disclosures or acquisitions of health information or private data to their immediate supervisor or the UF Privacy Office, (telephone numbers are posted on the UF Privacy Office website (<http://privacy.health.ufl.edu>) and in the UF & Shands Notice of Privacy Practices).
2. **Non-Retaliation:** Neither the University of Florida, nor any of its employees or business associates, shall discipline, or take any other adverse personnel action against an employee for any of the following actions:
 - a) *Reporting a violation or suspected violation of any federal, state, or local law, rule or regulation committed by an employee or business associate of the University;*
 - b) *Participating in an investigation, hearing, or other inquiry conducted by any agency of the state or federal government;*
 - c) *Refusing to participate in any adverse personnel action against an employee;*
 - d) *Initiating a complaint to their supervisor or the University's Office of Inspector General; or*
 - e) *Exercising any right established by University rules, policies or procedures.*
3. **Non-Compliance:**

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
HEALTH INFORMATION OPERATIONAL GUIDELINES

- a) *Members of UF's workforce who fail to comply with the University of Florida's privacy policies and procedures or with the requirements of the state and federal privacy regulations will be disciplined in accordance with the University of Florida's normal disciplinary procedures, up to and including termination of employment.*
- 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.*

4. Disclosures by whistleblowers. Neither the University, nor any of its workforce members, affiliated entities, or business associates shall be deemed to have violated the requirements of federal or state privacy regulations if the individual or entity discloses protected health information or personal identification information, provided that the individual or entity:

- a) *Reports unlawful conduct or suspected unlawful conduct which creates and presents a substantial and specific danger to the public's health, safety or welfare, in accordance with section 112.3187, Florida Statutes, (Florida's Whistle-blower's Act); or*
- b) *Has a good faith belief that the University or its workforce members, affiliated entities, or business associates have engaged in conduct which violates professional or clinical standards or University rules or policies; and*
- c) *The disclosure of information is to:*
 - (1) *An agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the University, or to an appropriate accreditation organization for the purpose of reporting the allegation of failure to meet professional standards; or misconduct by the University, its employees or business associates; or*
 - (2) *An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described above.*

5. Investigations and Disciplinary Action: The Privacy Officer or designee is responsible for investigating or for assisting with investigations of all suspected violations involving protected health information created and maintained by the University of Florida and its affiliated entities.

- a) *Every effort will be made to complete Investigations within 30 business days.*
- b) *The Privacy Officer recommends sanctions for confirmed violations to Department Chairs, considering the following factors:*
 - (1) *The facts of the investigation:*
 - (a) *The nature of the violation,*

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
HEALTH INFORMATION OPERATIONAL GUIDELINES

- a) *Step in to correct the situation, if possible. For example: interrupt an improper chat in an elevator; rescue a document left in a public place; or lock up an area with access to private data.*
- b) *If the breach involves a computer system containing private data:*
 - (1) Take immediate steps to secure the affected system. Follow departmental information security procedures.
 - (2) Report the breach, along with your contact information, immediately to your supervisor, your Unit Information Security Manager, and the appropriate UF Privacy Officer (Gainesville) or HIPAA Compliance Manager (Jacksonville).
 - (3) If a computer or other data management device has been lost or stolen, also notify the University Police Department, the Jacksonville Sheriff's Office, or your local law enforcement agency, as appropriate.

3. Reporting:

- a) *Incidental disclosures are not considered Privacy Incidents and do not usually need to be reported. However, members of the workforce should use professional judgment in assessing the potential outcome(s) of an incidental disclosure and report any disclosures that may result in a fraudulent or criminal misuse of the information or have a negative impact on the University of Florida or its affiliated entities.*
- b) *Accidental and intentional disclosures must be reported immediately to the Privacy Office.*
- c) *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 Protected Health Information and one for Private Data (other than health information).*
 - (1) Include the following information:
 - (a) *Date, time and location of the incident: time may be estimated; location should be the College, Department, Division, Clinic or other Unit affected, or the location of found documents.*
 - (b) *The nature of the violation: A clear description of what happened and how, if known.*
 - (c) *Type of private data involved: Paper records, electronic records, or other type of data.*
 - (d) *Other persons involved: Names, titles, contact information, and how they were involved.*
 - (2) Any immediate harm known or observed: Was data disclosed, altered, damaged, or destroyed? Was the patient/client aware?
 - (3) Immediate corrective actions already taken: for example, documents or computer equipment secured, recipient of PHI asked to return or destroy the data, misdirected e-mail retracted.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
HEALTH INFORMATION OPERATIONAL GUIDELINES

d) *Send the Privacy Incident Report to the Privacy Office immediately.*

- (1) For UF-Gainesville, all FGP / UFP Clinics, and all remote practice sites: send to UF-Gainesville Privacy Office
- (2) For UF-Jacksonville and all UFJPI/ UFJHI Clinics: send to UF-Jacksonville Office of the General Counsel and HIPAA Compliance.

4. **Follow Up:** After investigation, if notification of affected persons or mitigation is required, departments and/or individuals involved in the privacy breach may be asked to assist with the notification process and/or in mitigating harmful effects.

E. PROCEDURES FOR MANAGERS

1. **Responding to Complaints:** See the chapter on Complaints

2. **Responding to Loss or Inappropriate Disclosure of Information**

a) *Misplaced or Stolen Records: (For record recovery procedures, see Health Information and Record Management in the Operational Guidelines.)*

- (1) If every effort has been made to retrieve a lost record and it has been determined that retrieval is unlikely, log the loss into the Disclosure Tracking System as an accidental disclosure.
- (2) If a record that was believed to be lost or was known to have been stolen is later recovered, do not attempt to alter the entry in the Disclosure Tracking System.

b) *Inappropriate Disclosures: Information mailed or faxed to incorrect address or wrong individual:*

- (1) Make every effort to retrieve the information that was sent (have it mailed back or hand-carried), or get assurance from the recipient that it was destroyed. Document these efforts and the results on the Incident Report form.
- (2) Log the disclosure into the Disclosure Tracking System.
- (3) Indicate on the Incident Report form 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.

F. REFERENCES:

1. **HIPAA:** 45 CFR §164.530 (e) and (f) (Sanctions and Mitigation)
2. **Florida Administrative Code:** Rules 6C1-1.008(1)(o), 6C1-3.047(3)(d), 6C1-4.016(2)(o) and (t), and 6C1-7.048(1)(c)
3. **Florida Statutes:** 817.568 & 817.5681 (Criminal use of personal information)

G. EXHIBITS: None