

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
PRIVACY MANAGEMENT

Investigating and Responding to Privacy Violations

□ POLICY

Rev: 01/01/2008

1. The University of Florida will investigate and attempt to resolve all complaints and confirmed incidents relating to breaches of privacy and confidentiality within a reasonable time after a complaint is received or a privacy incident is reported.
2. The University of Florida will not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person filing a complaint or reporting a privacy incident, or inquiring about how to file a complaint or incident report.
3. The University of Florida may not require patients to waive their rights to file a privacy complaint as a condition for providing health care, arranging for payment for health care, enrollment in a health plan, or eligibility for health care benefits.
4. The University of Florida will designate staff to review and determine action on privacy complaints and incident reports filed with the University. These designated staff will also perform these functions when the University of Florida is contacted about complaints filed with the Office of Civil Rights.
5. The University of Florida will document all privacy complaints and reported privacy incidents.
 - a. Documentation will include:
 - 1) The findings from reviewing each complaint and incident,
 - 2) A description of corrective actions taken, or an explanation of why corrective actions are not needed,
 - 3) A description of risk assessments completed when restricted or sensitive data is involved,
 - 4) Any notification procedures taken, including recommendations and final approvals, and
 - 5) Any mitigation undertaken for each specific complaint or incident.
 - b. Documentation for all privacy complaints and incidents will be maintained for at least six years, or longer if required by law or other circumstances.
6. The University will make reasonable efforts to notify affected persons if it is determined that their personal identification information was, or is reasonably believed to have been, acquired by an unauthorized person and that the information could be used for fraudulent purposes. Notification to affected individuals will include the following components. The notification will also be posted on the UF Privacy website, if appropriate.
 - a. A general description of the incident;
 - b. The Police Report number, if available,
 - c. Instructions and necessary information for notifying the major credit agencies of suspected or potential identity theft.
 - d. The University's Privacy Office telephone numbers, including the Hotline, and website information.

□ PRIVACY DEFINITIONS

Breach: An actual violation of policy or procedure; going against established rules. Also, an unlawful and unauthorized acquisition of data that materially compromises the security, confidentiality, or integrity of personally identifiable information maintained by an entity.

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

Investigating and Responding to Privacy Violations (continued)

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.

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.

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.

Privacy Incident: A known or suspected action, inconsistent with the organization's privacy policies and procedures, or an adverse event, related to restricted or sensitive information.

□ IT DEFINITIONS FOR PRIVACY

Access (to Information): The ability or the means necessary to read, write, modify, or communicate data or information or otherwise make use of any system resource.

Authorized Access: Rights granted to an individual to allow access to information.

Authorized Disclosure: The permissible release, transfer, provision of, access to, or, divulging in any other manner of information by any means of communication outside the entity holding the information.

Compromise: Access in excess of that intended to be available.

Data Processing Software: the programs and routines used to employ and capabilities of data processing hardware, including but not limited to, operating systems, compilers, assemblers, utilities, library routines, maintenance routines, applications of networking programs.

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.

Information Technology Resources (Florida Chapter 119.011): IT Resources means data processing hardware and software communications, supplies personnel, facility resources, maintenance, and training.

IT Resource: Any equipment that has the primary purpose to store, process, display or transport digital information. The associated data, applications and hardware, are also IT resources.

Need-to-Know: Approved access to, or knowledge or possession of specific information required to carry out official duties by officers and employees of the enterprise that maintains the data.

Reasonable Person Standard (agreed to 5-8-06): Phrase to denote a hypothetical person who exercises qualities of attention, knowledge, intelligence and judgment that society requires of its members for the protection of their own interest and the interest of others. (i.e. A test for negligence is based on either a failure to do something that a reasonable person, guided by considerations that ordinarily regulate conduct, would do, or on the doing of something that a reasonable person would not do.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
PRIVACY MANAGEMENT

Investigating and Responding to Privacy Violations (continued)

Risk of Potential Harm: Undesired consequences of an action or event, capable of developing into an actuality, that causes physical or psychological/emotional damage to an individual. Harm is any detriment caused by a violation of a legal interest, as a result of a certain technical process or state.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operation, in an information system.

Valid Business Purpose: Assigned job activities that provide a requirement to use your authorized access to view, read, modify, possess, or communicate data or information.

□ PRIVACY REQUIREMENTS

1. A person who believes the University of Florida is not complying with the requirements of federal or state privacy regulations may file a complaint with the University's Privacy Officer. If PHI is involved, a Health Information privacy complaint may also be filed with the U.S. Secretary of Health and Human Services. (See: Operational Guidelines: Complaints)
2. The University must provide a process for individuals to make complaints or to report incidents regarding the University's information privacy and security procedures. The University must document all complaints and privacy incident reports received and their disposition.
3. The University must notify any resident of the State of Florida of any breach of the security of a computerized data system that includes unencrypted personal information, if it is determined that the information was, or is reasonably believed to have been, accessed by an unauthorized person.
4. The University must apply appropriate sanctions against members of its workforce who fail to comply with the University's privacy and security policies and procedures or with federal and state privacy and security regulations.
5. The University must mitigate, to the extent practicable, any harmful effect of a confirmed health information privacy violation.

□ PROCEDURES:

1. *Investigating Privacy Complaints and Privacy Incidents:*
 - a. Privacy Complaints: The Privacy Officer or designated representative will -
 - 1) Initiate a formal investigation immediately upon receipt of a formal verbal complaint or a completed Privacy Complaint form.
 - 2) Contact the complainant, preferably by telephone, within three (3) business days of receiving notice of a formal complaint.
 - a) Document the conversation, including the date, time, and a general summary of the conversation.
 - b) If a voice mail is left, continue to pursue direct communication.
 - 3) Attach any relevant materials or statements to the investigation documents.
 - 4) File the completed Privacy Complaint form along with all investigation and resolution documentation in the Privacy Office. If the complainant is a patient, student, employee, or otherwise associated with the University, the documentation is not included in the complainant's personal medical, personnel, or academic records.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
PRIVACY MANAGEMENT

Investigating and Responding to Privacy Violations (continued)

- 5) Maintain all documentation for at least six years.
 - b. Privacy Incidents: The Privacy Officer or designated representative will -
 - 1) Initiate a formal investigation immediately upon receipt of a report of a Privacy Incident. The person notifying the Privacy Office should complete a Privacy Incident Report form for this purpose.
 - 2) Determine whether the person(s) whose information is involved is aware of the alleged incident:
 - a) If the person/s is/are aware of the incident, contact them within three (3) business days of receiving notice of the incident. The method of contact is at the discretion of the Privacy Officer. Document the contact, and include the date, time and a general summary of any conversations or messages left or received.
 - b) If the affected persons are not aware of the privacy incident, investigate the alleged incident thoroughly before determining whether they should be informed. (See *Actions to be Taken When a Privacy Violation is Found*, following.)
 - 3) File the completed Privacy Incident form with all investigation and resolution documentation in the Privacy Office. If the person whose information is involved is a patient, student, employee, or otherwise associated with the University, the documentation is not included in their personal medical, personnel, or academic records.
 - 4) Maintain all documentation for at least six years.
2. *Actions To Be Taken By the Privacy Officer When No Privacy Violation Is Found*
- a. Documentation: If after investigation of either a complaint or an incident, it is determined that none of the federal or state privacy or security regulations or the privacy/security policies of the University of Florida have been violated, document the findings in appropriate reports and summarize the findings and recommended actions (if any).
 - b. Notification:
 - 1) For Privacy Incidents where no violation is found, only notify the person whose information was involved if they were already aware of the potential violation and that it was being investigated. Document any conversations, and provide written records of the incident resolution, as appropriate.
 - 2) For Privacy Complaints where no violation is found, notify the complainant upon conclusion of the investigation and explain the findings; provide a written record of the complaint resolution.
 - a) Document the response to the notification, specifically, whether the person was satisfied or dissatisfied with the disposition of the complaint/incident.
 - b) If the person is not satisfied, refer the matter to the University of Florida's legal counsel as well as any other University personnel directly involved, as necessary and appropriate.
3. *Actions To Be Taken By the Privacy Officer When A Privacy Violation Is Found*
- a. Documentation: If after investigation it is determined that state or federal regulations or the privacy/security policies of the University of Florida have been violated document the findings in appropriate reports and summarize the findings and recommended actions.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
PRIVACY MANAGEMENT

Investigating and Responding to Privacy Violations (continued)

- b. Corrective Action: Convene and direct the panel of University of Florida expertise, appointed to recommend a corrective action and recovery plan, including any plans for mitigation, where appropriate.
 - c. Notification: Privacy Complaints:
 - 1) Upon conclusion of the investigation, meet with or contact the complainant and explain the findings; provide a written record of the complaint resolution.
 - 2) Document the complainant's response (whether the complainant is satisfied or dissatisfied with the disposition of the complaint).
 - 3) If the complainant is not satisfied with the disposition of the complaint, refer the matter to UF's legal counsel and any other University personnel directly involved (if necessary and appropriate).
 - d. Notification: Privacy Incidents
 - 1) Determine if notification is required:
 - a) Using the Risk Assessment procedure (following), the Privacy Officer determines whether notification is necessary and proceeds as determined.
 - b) When required, the Privacy Officer convenes the Core Notification Recommendation Group. Using the Notification Risk Assessment Procedure and the Notification Matrix, they determine together whether notification of the affected individuals is necessary. (See the Notification Risk Assessment Procedure, following.)
 - 2) If the person(s) whose information was involved is not to be notified of the confirmed privacy incident, the Privacy Officer documents the details of this decision.
 - 3) Notify affected individuals of the confirmed privacy violation in writing as follows:
 - a) Notify the appropriate UF Administration, as well as Public Relations, News & Communications, Risk Management, and the Vice President for Human Resources, immediately.
 - b) Assist the College, Department, Division, Clinic, or other University unit to notify all affected persons (patients, students, employees, legal representatives, etc.) as soon as is practicable.
 - (1) Notification must conform to the requirements of F.S. 817.5681.
 - (2) While the Privacy Office will oversee the notification process, the College, Department, Division, Clinic, or other University unit from which the information was acquired will be responsible for costs and labor associated with notifying the affected persons.
 - c) Document all subsequent conversations with the affected individuals, and provide them with written records of the incident resolution, as appropriate.
4. *Notification Risk Assessment Procedure*: Use the following process in making a 'notification' decision following an actual or suspected disclosure of Restricted information.

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
PRIVACY MANAGEMENT

Investigating and Responding to Privacy Violations (continued)

- a. Notification Recommendation Team:
 - 1) Core Members
 - a) University News and Public Relations
 - b) UF Chief Information Officer
 - c) UF IFAS Chief Information Officer
 - d) UF HSC Chief Information Officer
 - e) UF Privacy Office
 - 2) Ex-officio: Office of General Counsel
 - 3) Ad hoc
 - a) University Police Department
 - b) UF Information Security Forensic Team
 - c) UF Data Principal of the information related to the investigation
- b. Impact Considerations: Consider the impact to UF assets such as its financial assets (costs), its reputation, and in extreme cases the freedom of a workforce member in the event of an incident with criminal implications.
 - 1) Cost and Liability Considerations:
 - a) Legal and liability expenses (reserves)
 - b) Restitution for loss (victim financial damages)
 - c) Operational expenses to handle fallout, to resume business operation, etc.
 - d) Sanctions, fines, penalties assessed
 - e) Opportunity losses (donations, grants)
 - f) Potential for indictment and incarceration
 - 2) Reputation Considerations:
 - a) Damage to victims (sensitive nature of the data)
 - b) Whether the reputation damage to UF will be minimal, short term or long term
 - 3) Media and Public Interest Considerations:
 - a) Local – community, county, Gainesville and Jacksonville
 - b) Regional – State wide or south eastern US
 - c) National news interests
- c. Probability Considerations: Consider evidence of the intruder's capabilities for accessing the data, evidence of opportunity to access and/or use the data, and evidence of the intruder's intention to access and/or use the data.
 - 1) Capability of intruder or unauthorized accessor:
 - a) Privileges the intruder was able to assume
 - b) Footprints of intruder – activity, files installed
 - c) Adequacy of controls that were in place at the time of the breach
 - 2) Opportunity for intruder or unauthorized accessor to access:
 - a) Privileges the intruder was able to assume
 - b) Duration of intruder's presence on the system
 - c) Duration of intruder's activities
 - d) Access date/time stamps of Restricted and Sensitive data
 - 3) Intent or motivation of intruder or unauthorized accessor:
 - a) Misuse of computer resources
 - b) Data theft
 - c) Hardware theft
 - d) Thrill

UNIVERSITY OF FLORIDA
INFORMATION PRIVACY POLICIES & PROCEDURES
PRIVACY MANAGEMENT

Investigating and Responding to Privacy Violations (continued)

- 4) Misplaced data considerations (i.e. data on removable media or portable computer):
 - a) Accidentally discarded (type of media will be a factor; discarded hard drive or memory stick is more likely to result in an unauthorized disclosure than a discarded CD, DVD or floppy disk.)
 - b) Location is forgotten (again media will be a factor; misplaced laptop or PDA is more likely to result in an unauthorized disclosure than misplaced removable media.)
 - c) Recovery likelihood
- d. Risk Descriptions and Recommended Actions
 - 1) High: The risk analysis indicates high risk to the institution if it does not notify the victims. Privacy Officer and/or Core Team must recommend notification.
 - 2) Moderate: The risk analysis indicates risk to the institution if it does not notify the victims.
 - a) Consider notifying if the institution believes the breach may reach the public and it wishes to pre-empt with facts for damage control.
 - b) Notification recommendation is determined by a consensus of the Core Team with dissenting opinion going forward with the recommendation.
 - 3) Low: The risk analysis indicates a low risk to the institution if it does not notify the victims. The Privacy Officer and/or Core Team may still recommend notification.
- e. Recommendations and Final Approval: Upon completion of the recommendation the Core Team forwards it to the Senior Vice-President for Administration for approval, unless functional responsibility is specifically delegated (i.e., Chief Privacy Officer).

REFERENCES

HIPAA Regulations: 45 CFR § 160.306 (Complaints to the Secretary) and § 164.530(d) (Complaints), (e) (Sanctions), and (f) (Mitigation)

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)

UF Privacy Policy & Procedure Manual - Operational Guidelines: Privacy Investigation Flowchart, Recommended Corrective Actions and Sanctions Matrix

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

- ### EXHIBITS:
- Privacy Violation Flowchart
 - Notification Flowchart
 - Sample Notification Letters (2)
 - Article from Federal Trade Commission website
 - Forms: Privacy Incident / Complaint Summary Report and Follow-up Report