

## SECTION 6: OTHER PRIVACY POLICIES AND PROCEDURES

### 6.7 Identity Theft Prevention Program

#### POLICIES

1. **Commitment:** The University of Florida (UF) will make every reasonable attempt to protect the personal identification and personally identifiable financial information it creates, receives, maintains, and transmits, and to comply with current laws that provide for the protection of these types of information.
2. As allowed and/or required by law, UF will collect, maintain, use, and disclose Social Security Numbers (SSNs) and credit card or other financial information of employees, students, clients, patients, vendors, and others in the ordinary course of its business.
3. **Implementation of the Identity Theft Prevention Program and Compliance:** Each UF unit with access to personal identification or personally identifiable financial information is responsible for developing and implementing procedures to comply with the Identity Theft Prevention Program.
4. **Responding to a SSN Privacy Breach:** Workforce members must promptly report known or suspected loss or theft of SSNs from University records or record systems to the Privacy Office for immediate investigation. The unit manager/designee will determine whether the activity is fraudulent and will enlist the assistance of the Privacy Office.

#### DEFINITIONS

1. **Account** means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:
  - a. An extension of credit, such as the purchase of property or services involving a deferred payment; and
  - b. A deposit account.
2. **Consumer report:** means any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (a) credit or insurance to be used primarily for personal, family, or household purposes; (b) employment purposes; or (c) any other purpose authorized under section 604 [§ 1681b].
3. **Covered Account** means:
  - a. An account that the University of Florida offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, student account, or other financial accounts; and
  - b. Any other account that the University offers or maintains for which there is a reasonably foreseeable risk to Customers (Consumers) or to the safety and soundness of the institution from identity theft, including financial, operational, compliance, reputation, or litigation risks.
4. **Credit** means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

5. **Creditor**, as defined by the Red Flag Program Clarification Act of 2010, means one that regularly and in the ordinary course of business:
  - a. Obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;
  - b. Furnishes information to consumer reporting agencies, as described in section 623, in connection with a credit transaction; or
  - c. Advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person (i.e., student financial aid or Gator1 debit cards); this does not include a creditor that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person; and
  - d. (Includes any other type of creditor... based on a determination that such creditor offers or maintains accounts subject to a reasonably foreseeable risk of identity theft.
6. **Customer (Consumer)** means a person that has a Covered Account with the University of Florida.
7. **Identity Theft (16 CFR 603.2(a))** means a fraud committed or attempted using the identifying information of another person without authority. In a medical setting, Identity Theft may involve using a patient's name and/or insurance information without the patient's knowledge to fraudulently obtain medical services or benefits.
8. **Identifying information** means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:
  - a. Name, Social Security Number, date of birth, official state or government issued driver license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
  - b. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
  - c. Unique electronic identification number, address, or routing code; or
  - d. Telecommunication identifying information or access device.
9. **Records:** Any document, file, database, image, recording, or other means of expressing fixed information, made or received by an institution according to law or its particular mandate and preserved by it in any form as evidence or information.
10. **Record Systems:** All mechanisms and media used for input, storage, organization, display, retrieval, and printing of records. Systems consist of components including, without limitation, computers, computer peripherals, wired and wireless networks used for voice and data, as well as fax machines, photo copiers or paper, and paper filing systems.
11. **Red Flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
12. **Restricted data:** Data in any format collected, developed, maintained or managed by or on behalf of UF, or with the scope of UF activities that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to, medical records, social security numbers, credit card numbers, Florida driver licenses, and export controlled data.
13. **Service provider** means an organization, business, or person that provides a service directly to UF. Examples include billing of customers, collecting debt, and managing accounts.

14. **Workforce** means UF faculty, staff, students, volunteers, and any other persons under the direct control of UF, whether temporary or permanent, paid or not paid; also including, but not limited to, visiting and associate clinicians, faculty, students, and other persons performing services for UF.


**PRIVACY REQUIREMENTS**

1. Social Security Numbers

- a. Classification: Social Security Numbers obtained by the University are classified as Restricted Data and must be protected from unauthorized use or disclosure.
  - i. Security protocols, including those for any hardware and software housing restricted data, will be subject to audit by the University's Office of Internal Audit and Information Security Office.
  - ii. In limited circumstances, with documented approval from the Privacy Office, individuals and units may be allowed to use Social Security Numbers or truncated (last four digits) Social Security Numbers for certain specific purposes.
- b. Collection or Use of SSNs :
  - i. The University of Florida, as a State agency, may not collect an individual's SSN unless it has stated in writing its purpose for the collection and unless it is: a) specifically authorized by law to do so, or b) imperative for the performance of the University's duties and responsibilities as prescribed by law.
  - ii. SSNs collected by the University may not be used for any purpose other than the purpose for which it is authorized and provided in the written statement.
  - iii. Authorized uses of SSNs include:

Tax Reporting - required as a taxpayer ID for all tax information reported to the IRS, including: <ul style="list-style-type: none"> <li>• Wage and withholding data for full-time and part-time employees,</li> <li>• Honoraria provided to guest lecturers,</li> <li>• Independent contractors working for the University,</li> <li>• Payments to research participants for 1099s.</li> </ul>
Financial Aid - to obtain federal financial aid information and to identify and confirm the level of financial aid assistance.
Human Resource Services - approved for use on federal I-9 forms for hiring purposes, employment verification, and by certain benefit providers, such as insurance companies for verification of eligibility and coordination of benefits.
Law Enforcement - Federal and state agencies often rely upon SSN's as the primary identifier for law enforcement and criminal information purposes. In the event such agencies request SSN information using proper procedures, it will be provided following review and approval through the Privacy Office in consultation with the Office of the General Counsel.
Patients – approved for verification of health insurance coverage, to determine eligibility and coordination of other related benefits, and to aid in collections.
Business Imperatives of the University: <ul style="list-style-type: none"> <li>• Identity Management - to maintain the integrity of student records and verify the identities of students and workforce members.</li> <li>• External Reporting - to fulfill the University's responsibility to provide transcripts and other information, such as regulatory reporting, for which more universally known IDs are required.</li> </ul>

- iv. Any unit collecting or using SSNs for purposes other than those authorized or prescribed by law must obtain written approval from the Privacy Office. See 6.5 Collect or Use of SSNs policy.
- v. The Privacy Office maintains a list of University units that are authorized to collect or use SSNs and their statutory authority to do so. Any unit of the University collecting an individual's Social Security Number shall provide that individual with a copy of the written statement required below.

	<b>Date:</b> _____
<b>Department Name:</b> _____	
<b>COLLECTION AND USE OF SOCIAL SECURITY NUMBER</b>	
<b>Your Social Security Number has been collected because:</b>	
<input type="checkbox"/>	<b>This department is specifically authorized by law to do so.</b>
<input type="checkbox"/>	<b>It is imperative for the performance of this department's duties and responsibilities as prescribed by law.</b>
<b>If you have questions about the collection and use of Social Security Numbers, please visit:</b>	
<b><a href="http://privacy.ufl.edu/SSNPrivacy">http://privacy.ufl.edu/SSNPrivacy</a></b>	

- c. Training: Workforce members, including students and volunteers, who have access to SSNs must complete Social Security Number privacy training during their initial orientation and annually, thereafter.
  - i. Online training, Protecting SSNs, is available through myTraining.
  - ii. Unit supervisors/unit administrators are responsible for implementing appropriate unit training requirements based on the job duties of workforce members in the unit.
- 2. Financial and Consumer Information: If a University unit is a Creditor and maintains Covered Accounts (see Definitions above), the unit must develop and implement procedures to comply with the Identity Theft Prevention Program.
  - a. Program Administration
    - i. The Identity Theft Prevention Program is the responsibility of the University of Florida's Board of Trustees, which will approve the initial program, recertify the program every two years, and maintain appropriate documentation of the program and its subsequent amendments.
    - ii. The University's Privacy Office maintains operational responsibility for the oversight, development and administration of the Program.
  - b. Detecting Red Flags: Workforce members should be alert for Red Flags, which are potential indicators of identity theft or other fraudulent activities. A Red Flag, or any situation closely resembling a Red Flag, should be investigated for verification. The following are examples of Red Flags. Additional examples are provided in the Exhibits at the end of this policy.
    - i. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
    - ii. The presentation of suspicious documents;
    - iii. The presentation of suspicious personal identifying information, such as a suspicious address change;
    - iv. The unusual use of, or other suspicious activity related to, a Covered Account; and

- v. Notice from Customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts held by the financial institution or creditor.
- c. Responding to Red Flags and Identity Theft: Known and suspected fraudulent activity must be reported immediately to protect Customers and the University from damages and loss.
  - i. Gather all related documentation and complete a Privacy Incident Report, available on the Privacy Office web site; provide a complete description of the situation. Send the report to the UF Privacy Office.
  - ii. If, after investigation, a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:
    - Canceling the transaction;
    - Notifying and cooperating with appropriate law enforcement;
    - Determining the extent of liability of the University; and
    - Notifying the Customer that fraud has been attempted.
- d. Violations: Corrective action will be taken in the event of intentional violations of this policy. Such action may include:
  - i. Reevaluation or modification of policies, procedures or workflows in order to enhance the protection of personal identification or personally identifiable financial information, and/or
  - ii. Disciplinary action up to and including termination or expulsion in accordance with University policies.
- e. Training: University workforce members who have access to consumer reports and/or covered accounts must complete Identity Theft and the Red Flags Rule training at hire, and annually thereafter. Workforce members should also be familiar with their respective unit's Identity Theft Prevention procedures.
- f. Updates to the Identity Theft Prevention Program: The Program will be reevaluated every two years, or as otherwise required to include:
  - i. An overview of all aspects of the Program to be sure they are up to date and applicable in the current business environment.
  - ii. An assessment of the types of covered accounts that UF offers or maintains.
  - iii. Revision, replacement or elimination of Red Flags to reflect previous experience with and emerging risks or threats of identity theft.
  - iv. Review of corrective actions, sanctions, and mitigation plans.
- g. Oversight of Service Provider Arrangements
  - It is the responsibility of University units that engage a service provider to perform an activity in connection with one or more covered accounts to ensure that the activities of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

- A service provider that maintains its own identity theft prevention program, consistent with the guidance of the Red Flags Rule, validated by appropriate due diligence, and included in the service agreement, may be considered to be meeting these requirements.
  - Any specific requirements should be specifically addressed in the appropriate contract arrangements.
- h. Security: The University will implement every reasonable measure to protect restricted data provided to it by individuals, including, but not limited to, creating, maintaining, and using University records and record systems securely so that restricted data are only used and disclosed in accordance with state and federal regulations.
- i. Prohibited Activities:
- i. Public display of restricted data. (i.e., to exhibit, hold up, post, or make visible or set out for open view, including but not limited to, open view on a computer device, computer network, website, or other electronic medium or device, to members of the public or in a public manner.)
  - ii. Using restricted data as the primary account number or identifier for an individual, except where existing University records or record systems require such use. Existing records or records systems, when retired, will be replaced with records or record systems that do not require or use SSNs or credit card numbers as the primary account number or identifier.
  - iii. Visibly printing restricted data on identification cards or badges
  - iv. Using, transmitting by any means, including by email, downloading, or storing restricted data in or from records, record systems, or databases that are not encrypted or otherwise secured.
- j. Limited Access: Only properly authorized users will be provided access to records and record systems containing restricted data. Access is granted in accordance with the user's employment or professional responsibilities and is limited to those who have an approved business reason to use or disclose this information.
- k. Record Disposal: Records containing restricted data must be disposed of in a manner that minimizes the risk of unauthorized access to or use of the records when those documents no longer need to be retained and pursuant to University document retention policies.
- i. Paper documents containing restricted data should be shredded immediately, or placed in secure containers for shredding later by a licensed document destruction company.
  - ii. Record systems and/or electronic media containing restricted data will be sanitized or destroyed in a manner approved by the Information Security Office prior to reuse, repurposing, or when no longer needed.

## REFERENCES

1. Florida Statutes: F.S. 119.071(5) General exemptions from inspection or copying of public records; F.S. 817.568 Criminal use of personal identification information
2. 15 U.S.C. 1681 et seq.: Fair Credit Reporting Act
3. 18 U.S.C. 1029(e): Fraud and related activity in connection with access devices
4. Title 16 CFR – Commercial Practices: Part 681 Identity Theft Rules
5. 12 CFR 1022.3 Fair Credit Reporting (Regulation V) - Definitions
6. 12 CFR 334.82: Fairness and Accuracy in Credit Transactions Act

- 7. Red Flag Program Clarification Act of 2010
- 8. UF Regulations: 1.0103 Policies on Restricted Data
- 9. UF Information Security Data Classification Policy

**EXHIBITS**

1. Red Flag Indicators Table

<b>Red Flag Indicators</b>	
<b>Alerts, notifications or warnings from a consumer reporting agency:</b>	<ul style="list-style-type: none"> <li>• A fraud or active duty alert included with a consumer report;</li> <li>• A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;</li> <li>• A notice of address discrepancy from a consumer reporting agency</li> </ul>
<b>Consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or Customer:</b>	<ul style="list-style-type: none"> <li>• A recent and significant increase in the volume of inquiries;</li> <li>• An unusual number of recently established credit relationships;</li> <li>• A material change in the use of credit, especially with respect to recently established credit relationships;</li> <li>• An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.</li> </ul>
<b>Suspicious Identification (ID) or Application Documents:</b>	<ul style="list-style-type: none"> <li>• Documents provided for ID that appear to have been altered or forged.</li> <li>• Photo or physical description on the ID is not consistent with the appearance of the person presenting it.</li> <li>• Other information on the ID is not consistent with information provided by the person presenting the ID or with readily accessible information that is on file, such as a signature card or a recent check.</li> <li>• An application appears to have been altered, forged, or destroyed and reassembled.</li> </ul>

**Red Flag Indicators**

**Suspicious Personal Identifying Information (PII):**

- PII provided is inconsistent when compared against external information sources. For example,
  - The address does not match any address in the consumer report;
  - The SSN has not been issued or is on the Social Security Administration's Death Master File; or
  - Personal identifying information provided by the Customer is inconsistent.
- PII provided is associated with known fraudulent activity. For example,
  - The address given is the same as one provided on a fraudulent application.
- PII provided is of a type commonly associated with fraudulent activity. For example:
  - The address on an application is fictitious, a mail drop, or a prison; or
  - The phone number is invalid or is associated with a pager or answering service.
- The SSN provided is the same as that submitted by other persons or Customers.
- The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other Customers or other persons opening accounts.
- The Customer or the person opening the Covered Account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- PII provided is not consistent with PII on file.
- The person cannot provide authenticating information for security questions (mother's maiden name, pet's name, etc., beyond that which generally would be available from a wallet or consumer report.



**Red Flag Indicators**

**Unusual or Suspicious Activity**

- Shortly following the notice of a change of address for a Covered Account, a request is received for new, additional, or replacement goods or services, or for the addition of authorized users on the account.
- A new revolving credit account is used in a manner commonly associated with known patterns of fraud.
  - The Customer fails to make the first payment;
  - The Customer makes an initial payment but no subsequent payments.
- A Covered Account is used in a manner inconsistent with established patterns of activity on the account.
  - Nonpayment when there is no history of late or missed payments;
  - A material change in purchasing or usage patterns;
  - A material change in EFT patterns in connection with a direct deposit account.
- A Covered Account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
- Mail sent to the Customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the Customer's Covered Account.
- Notification is received that the Customer is not receiving paper account statements, or of unauthorized charges or transactions in connection with a Customer's Covered Account.
- Notification is received from Customers, victims of identity theft, law enforcement authorities, or any other persons regarding possible identity theft in connection with Covered Accounts held by UF, or that UF has opened a fraudulent account for a person engaged in identity theft.