University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

ADMINISTRATIVE POLICY STATEMENT

Policy Title: Collection of Personal Data from Students and Customers

APS Number: 7003 **APS Functional Area:** **RISK MGMT/PUBLIC SAFETY**

Brief Description:	Sets forth requirements for the collection of personal data from students and other customers of the University, and for detecting warning signs associated with identity theft.
Effective:	July 1, 2009
Approved by:	President Bruce D. Benson
Responsible University Officer:	Office of Vice President for Finance
Responsible Office:	Office of University Controller
Policy Contact:	Office of University Controller
Supersedes:	Collection of Personal Data from Students and Customers, July 1, 2007
Last Reviewed/Updated:	July 1, 2009
Applies to:	All campuses

Reason for Policy: To set forth requirements for the collection of personal data from students and steps to be followed by organizational units when conducting business with students.

I. INTRODUCTION

This policy sets forth requirements for the collection of personal data from *students*, including medical residents, and customers for use in various business and regulatory processes, including but not limited to Internal Revenue Service reporting, collection efforts, and student insurance and medical services It further sets forth requirements that must be followed by *organizational units* when conducting business with *students*, including medical residents, and other customers of the University. These requirements include detecting the warning signs, or "red flags," of identity theft in day to day operations and taking steps to prevent a red flag from escalating into an episode of identity theft.

II. POLICY STATEMENT

A. Required and Preferred Personal Data

The following are considered to be required personal data that must be collected in accordance with these procedures:

1. Individual's legal name;
2. Social Security Number and/or Federal Employer Identification Number;
3. Permanent address; and
4. Date of birth.

The following data is encouraged (but not required) to be collected where applicable and cost-effective to do so:

1. Current home and work address;
2. Current home and work phone number; and
3. Name and address of nearest relative or guardian not living with customer/student.

B. Collection Requirements

The collection of personal data from *students*, including medical residents, and *customers* of the University is a sound business practice and is required per this policy for:

1. *students* and *customers* with either a *formal credit relationship* or informal credit relationship with the University;
2. medical residents providing training services at a *medical affiliate*; and
3. *students* applying for federal financial aid for which the University is the creditor and state financial aid[1].

The required personal data will be collected when an individual initiates the credit relationship, financial aid request, or medical resident training agreement.

The required and preferred personal data (identified in Section A, above) will be maintained in accordance with the IT Administrative Policy Statement referenced in Section III.A., below.

C. Collection Requirement Exemptions

An informal credit relationship is created when the University receives an insufficient fund check or a credit card chargeback. These informal credit relationships are exempted from the requirements of this policy, but *organizational units* must comply with applicable policies issued by the University Treasurer that pertain to receiving payments by checks and credit cards.

The University has a few services, such as parking, that are provided without registration or that demonstrate minimal collection risk. An *organizational unit* may obtain an exemption from collection requirements for these services from the appropriate campus Controller.

A *customer* (but not a *student* applying for financial aid or a medical resident entering into a training agreement) may request an exemption from providing her/his Social Security Number and/or Federal Employer Identification Number by paying for the requested services in full prior to receiving any part of the service. The exemption may be requested from the responsible *organizational unit*.

If an exemption is not granted and the personal data are not collected in accordance with this policy, then the goods, service, or financial aid may not be delivered to the *customer*, *student,* or medical resident. It is the responsibility of the *organizational unit* to ensure procedures are in place so as to prevent delivery of the goods, service, financial aid or medical resident training agreements.

D. Potential Indicators (Red Flags) of Identity Theft

In order to identify potential identity theft, the University considers a number of factors including:

1. the types of accounts that it offers and maintains;
2. the methods used to open accounts; and
3. the methods used to provide access to accounts.

For purposes of this section, a covered account with respect to identify theft includes:

1. Any credit account the University offers or maintains for that involves multiple payments or transactions.
2. Any other account the University offers or maintains in which there is a reasonably foreseeable risk to the safety or soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

[1] State financial aid for the purposes of this policy includes stipend payments in the State of Colorado College Opportunity Fund.

Employees should be aware of and monitor for the following red flags when working with a transaction that involves a covered account:

1. **Notifications and Warnings from Credit Reporting Agencies**
    a. Alerts, notifications or warnings from a consumer reporting agency;
    b. A fraud or active duty alert included with a consumer report;
    c. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
    d. A notice of address discrepancy from a consumer reporting agency.
    e. Consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
        - A recent and significant increase in the volume of inquiries;
        - An unusual number of recently established credit relationships;
        - A material change in the use of credit, especially with respect to recently established credit relationships; or
        - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
2. **Suspicious Documents**
    a. Documents provided for identification that appear to have been altered or forged;
    b. Documents in which the photograph or physical description is not consistent with the appearance of the applicant or customer presenting the identification;
    c. Documents containing information that is not consistent with information provided by the person opening a new covered account or customer presenting the identification;
    d. Documents containing information that is not consistent with existing customer information on file with the *organizational unit*;
    e. Applications for services that appear to have been altered or forged, or give the appearance of having been destroyed and reassembled.
3. **Suspicious Personal Identifying Information**
    a. Personal identifying information provided is not consistent with personal identifying information that is on file with the *organizational unit*;
    b. Personal identifying information that is considered inconsistent when compared against external information sources used by the *organizational unit*. For example, the address does not match any address in the consumer report;
    c. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, inconsistent birth dates;
    d. Personal identifying information provided is associated with known fraudulent activity. For example, the address on an application is the same as the address provided on a fraudulent application;
    e. Personal identifying information 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 opening an account or by other 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.
    f. The customer or the person opening the covered account fails to provide all required personal identifying information on an application when requested.
    g. When using security questions (mother's maiden name, pet's name, etc.), the customer or the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
4. **Unusual or suspicious activity related to the covered account such as:**
    a. Shortly following the notice of a change of address for a covered account, the *organizational unit* receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.
    b. A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments.

c. An account which is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
   - Nonpayment when there is no history of late or missed payments;
   - A material change in purchasing or usage patterns

d. An 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).

e. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

f. The *organizational unit* is notified that the customer is not receiving paper account statements.

g. The *organizational unit* is notified of unauthorized charges or transactions in connection with a customer's covered account.

h. The *organizational unit* receives 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 *organizational unit*.

i. The *organizational unit* is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

E. Required Red Flag Procedures

When potentially fraudulent activity is detected, an employee must act quickly because a rapid and appropriate response can protect the University and its customers from damages and loss. Follow the steps below:

1. Gather all related documentation and write a description of the situation.
2. Present this information to the GLB (Gramm-Leach-Bliley) Compliance Officer for determination.
3. The GLB Compliance Officer will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

If 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 actual customer that fraud has been attempted.

III. PROCEDURES, FORMS, GUIDELINES, AND RESOURCES

A. Related Administrative Policy Statements

1. IT Security in University Operations, Continuity, and Contracting

B. Educational Resources

Educational resources including guides, training announcements, and newsletters are announced and available on Office of University Controller and Office of Information Security websites.

C. Related Policies and Laws

The Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act Gramm-Leach-Bliley Act of 1999

IV. DEFINITIONS

Italicized terms used in this Administrative Policy Statement are defined in the Administrative Policy Statement Policy Glossary.

V. CONTACTS

The appropriate campus Controller, consulting with the University Controller as appropriate, will respond to questions and provide guidance regarding interpretation of this policy. Any exceptions to this policy must be approved by the University Controller.

VI. HISTORY

Revised July 1, 2009
New July 1, 2007

VII. KEY WORDS

Red, flag, rule