University of Colorado **Anschutz Medical Campus**

Campus Administrative Policy Title

Policy Title: Safeguarding Customer Information

Policy Number: 7035A Functional Area: Student Affairs

Effective:	May 15, 2003
Date Last Amended/Reviewed:	May 15, 2003
Date Scheduled for Review:	July 1, 2010
Supersedes:	N/A
Approved by:	N/A
Prepared by:	N/A
Reviewing Office:	Provost Office
Responsible Officer:	Executive Vice Chancellor for Administration and Finance
Applies to:	CU Anschutz Medical Campus

A. Introduction

The purpose of this policy is to document the University of Colorado Anschutz Medical Campus (CU Anschutz) policy and procedures used to ensure all nonpublic personal customer information obtained by various CU Anschutz departments in the awarding of students loans is adequately safeguarded, protected, and is not shared with unauthorized individuals. The CU Anschutz Assistant Vice Chancellor for Finance/Controller is the campus designee responsible for coordination of the campus' information security under this policy and shall monitor compliance with this policy and update any changes or modifications to the procedures contained herein on an annual basis or as changes dictate.

This policy applies to all employees and departments involved in the "making, acquiring, or servicing of customer loans." The departments

covered under the policy are primarily the Student Financial Aid Office, Bursar's Office, and the Admissions Office. However, this policy also applies to any employees or units within a School or Central Services and Administration that may gather, transfer, or record nonpublic, personal customer information related to the making, acquiring, or servicing of a student loan.

B. Definitions

1. Customers: include students, faculty, or staff or that individual's legal representative who obtains or has obtained a financial product or service (e.g., loan) from CU Anschutz that is to be used primarily for personal, family, or household purposes.

   Examples include:

   a. An individual who provides nonpublic personal information to a CU Anschutz department in order to obtain a determination about whether they may qualify for a loan, regardless of whether the loan is extended.

   b. An individual who provides nonpublic personal information to a CU Anschutz department in connection with obtaining or seeking to obtain financial counseling or other advisory services is a consumer, regardless of whether the University establishes a continuing advisory relationship.

   c. If CU Anschutz holds ownership or servicing rights to an individual's loan, the individual is a customer, even if CU Anschutz holds those rights in conjunction with one or more other institutions.

   d. An individual who has a loan in which CU Anschutz has ownership or servicing rights is a customer, even if CU Anschutz hires an agent to collect on the loan.

2. Customer information:

   a. Personally identifiable nonpublic financial information; and

b. Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

C. Policy Statement

1. CU Anschutz, its faculty, staff, and students will not engage in the practice of selling, transferring, or in any other way disclosing nonpublic personal information of its customers.

2. The Assistant Vice Chancellor of Finance/Controller, as security coordinator of this policy, will hold a meeting no less than annually with the managers of the program areas covered by this policy to discuss potential risk areas associated with customer information covered under the GLB Act. Assessment of risks and development of adequate compensating controls will be developed as needed and incorporated into employee training as required.

Electronic Information stored in the Student Information System (SIS)

Nonpublic personal information of our customers, stored electronically with the Student Information System, is governed by a body of security policies and procedures promulgated, enforced, and maintained by System University Management Systems (UMS). UMS has issued a policy entitled UMS Information Security Program addressing the Gramm-Leach-Bliley Act and other regulations such as Federal Family Educational Rights and Privacy Act (FERPA). CU Anschutz will rely on the UMS program and security policies to ensure compliance with all GLB requirements as it relates to electronic data.

Manual Files and Hard-copy Customer Information

Student files in both the Student Financial Aid Office and Bursar's Office may also contain nonpublic personal information of CU Anschutz customers that is subject to this policy. In addition, the Admissions and Records Office keeps a manual file on students with loan deferments in its office that is subject to this policy. All of these records shall be maintained in locked filing cabinets or secure office areas that have restricted access. Access to manual files is only permitted to the employees of these work areas.

Third Party Service Providers

CU Anschutz uses a third party service provider for the administration of its student loans. CU Anschutz will ensure there is language in the contracts with all third party loan service vendors that ensures adequate security of nonpublic personal customer information under this policy.

Training

All employees working in the Student Financial Aid Office, Bursar's Office, and Admissions Office, will be trained on this policy and the security issues and risks associated with customer information. Employees of these areas will certify annually their understanding and compliance with this policy. Additionally, employees who have access to student data are required to comply with the CU Anschutz Data Security and Confidentiality Requirements (Exhibit A).

Notes

1. Dates of official enactment and amendments:
   May 15, 2003: Adopted
   May 2, 2019: Reformatted

2. History:
   May 2, 2019: Reformatted to reflect a Campus-wide effort to recast and revitalize Campus policy sites into a standardized and more coherent set of chaptered policy statements organized around the several operational divisions of the university. Article links, University branding, and formatting updated by the Provost's office.

3. Initial Policy Effective Date: May 15, 2003

4. Cross References/Appendix:
   • Standards for Safeguarding Customer Information, 16 CRF Part 314, promulgated
   pursuant to the Gramm-Leach-Bliley Act (GLB Act) (Pub. L. 106-102).
   • University Management Systems (UMS) policies:
   - UMS Information Security Program
   - University Data Security and Confidentiality Requirements
   - Access to Systems and Data

- Protection of Systems and Data