Published on *University of Colorado* (https://www.cu.edu)

GLBA Safeguards Rule: Examples of Nonpublic Personal Information [1]

The GLBA Safeguards Rule requires the University of Colorado to implement safeguards to ensure the security and confidentiality of certain nonpublic personal information (NPI) that is obtained when the University offers or delivers a financial product or service to an individual for personal, family, or household purposes. The Rule also covers any list, description, or other grouping of customers derived using NPI.

To comply with the rule, the University must implement an information security program that incorporates administrative, technical, and physical safeguards appropriate to its size and complexity, nature and scope of activities, and sensitivity of NPI at issue. The various administrative, technical, and physical safeguards implemented in connection with CU's comprehensive Data Governance [2] and Information Technology (IT) Security [3] programs are consistent with, and support, GLBA Safeguards Rule compliance.

Following are examples of NPI that may be obtained in connection with the delivery of a financial product or service:

- Account balances
- ACH numbers
- Bank account numbers
- Credit card numbers
- Credit ratings
- Date and/or location of birth
- Driver’s license information
- Income history
- Payment history
- Social Security numbers
- Tax return information
- Name, address, phone number on an application for financial aid

Following are examples of administrative, technical, and physical safeguards that may be implemented to protect customer information (NPI):

Administrative

- Check references or conduct background checks before hiring employees who will have access to customer information.
- Ask new employees to sign an agreement to follow University confidentiality and security standards for handling customer information.
- Limit access to customer information to employees who have a business reason to see it.
- Control access to sensitive information by requiring employees to use strong passwords

that must be changed on a regular basis and use password-activated screen savers to lock employee computers after a period of inactivity.
- Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. Consider that customer information in encrypted files will be better protected in case of theft of such a device.
- Regularly remind all employees of CU policy — and the legal requirement — to keep customer information secure and confidential.
- Develop policies for employees who telecommute.
- Impose disciplinary measures for security policy violations.
- Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.

Technical

- Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access.
- Take steps to ensure the secure transmission of customer information.
- Dispose of customer information in a secure way
- Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information.
- Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.
- Take steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach.

Physical

- Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.
- When customer information is stored on a server or other computer, ensure that the computer is accessible only with a strong password and is kept in a physically secure area.
- Maintain secure backup records and keep archived data secure by storing it off-line and in a physically secure area.

Groups audience:
Controller
Right Sidebar:
OUC - GLBA-Related Resources
OUC - GLBA-Need Help

Source URL:https://www.cu.edu/controller/glba-safeguards-rule-examples-nonpublic-personal-information

Links
[1] https://www.cu.edu/controller/glba-safeguards-rule-examples-nonpublic-personal-information
[2] https://www.cu.edu/ope/aps/6010 [3] https://www.cu.edu/ope/aps/6005