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

Gramm-Leach-Bliley Act (GLBA): Safeguards Rule [1]

Members of the University of Colorado community collect and use personal information for many educational and business functions. CU is committed to safeguarding this data consistent with applicable legal and policy requirements.

The GLBA Safeguards Rule [2]requires CU to implement safeguards to ensure the security and confidentiality of certain nonpublic personal information [3] (NPI) that is obtained when CU offers or delivers a financial product or service to an individual for personal, family, or household purposes. To support compliance with the Rule, CU has implemented administrative, technical, and physical safeguards as part of its comprehensive Data Governance [4] and Information Technology (IT) Security [5] programs.

Quick Look

What does the GLBA Safeguards Rule require?

The objectives of the GLBA Safeguards Rule are to:

- Ensure the security and confidentiality of customer information, including nonpublic personal information [3] (NPI).
- Protect against any anticipated threats or hazards to the security of such information.
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.

To comply, a covered institution must develop, implement, and maintain a *comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards* appropriate to the organization's size and complexity, nature, and scope of activities, and sensitivity of NPI at issue.

Requirements include:

- Designating an employee(s) to coordinate the information security program.
- Performing a risk assessment to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information (including NPI) that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assessing the sufficiency of any safeguards in place to control these risks. At minimum, the risk assessment must include consideration of risk in each relevant operational area, including:
    - Employee training and management.

    - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal.
    - Detecting, preventing, and responding to attacks, intrusions, or other systems failures.
- Implementing information safeguards to control identified risks and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures.
- Overseeing service providers by taking reasonable steps to select and retain providers capable of maintaining appropriate safeguards for NPI and requiring them by contract to implement and maintain such safeguards.
- Evaluating and adjusting the information security program in light of the results of the required testing/monitoring, any material changes to operations or business arrangements, or any other circumstances that may have a material impact on the program.

Note: *On April 4, 2019, the Federal Trade Commission (FTC) issued a Notice of Proposed Rule Making [6] (NPRM) proposing substantial changes to the Safeguards Rule. The proposed amendments to the Rule substantially increase the specific requirements an organization's information security program will have to meet. The public comment period on the proposed changes ended August 2, 2019, and the FTC held a public workshop to discuss the proposed changes in July 2020. The timing and scope of any amendment to the existing Rule is yet to be determined.*

Why does CU have to comply with the GLBA Safeguards Rule?

The Federal Trade Commission (FTC) is charged with administration and enforcement of the GLBA for financial institutions not regulated by other federal banking or finance-related authorities, including institutions of higher education (IHEs). The FTC has determined that most IHEs are "financial institutions" for purposes of the GLBA because "[m]any, if not all, such institutions appear to be significantly engaged in lending funds to consumers." 64 Fed. Reg. 33648 (May 24, 2000).

In addition, the Department of Education requires IHE compliance with the Safeguards Rule by contract, under the Federal Student Aid (FSA) Program Participation Agreement and Student Aid Internet Gateway (SAIG) Agreement.

How does CU comply with the GLBA Safeguards Rule?

CU is committed to safeguarding the personal information it collects, uses, or maintains for educational and business functions. This commitment is reflected in Regent Policy 8.A.7 Privacy and Confidentiality [7] and in the Administrative Policy Statement Code of Conduct [8], which describe the expectation that university community members will comply with applicable legal, contractual, and policy obligations to maintain the confidentiality of such information, protect it from improper disclosure, and protect the privacy interests of individuals.

To ensure that data is managed as a material asset and protected in compliance with

applicable requirements, CU has implemented a Data Governance Program [4] and adopted a suite of policies that establishes the university-wide IT Security Program [5] framework. Additional system-level and campus policies, procedures, and standards have been implemented to safeguard the confidentiality, integrity, and availability of information systems, services, and data in all forms, including personal information collected, maintained, or disposed of by CU or by service providers on CU's behalf.

CU's GLBA Safeguards Rule Information Security Program incorporates existing university policies, procedures, standards, and is in addition to any institutional policies and procedures that may be required under other federal and state laws and regulations.

How do I know if my org unit must comply?

Organizational units that collect/maintain NPI that must be safeguarded are typically involved in the provision or servicing of student, faculty, or staff loans, other extensions of credit, and collection agency services.

If your org unit collects, processes, maintains, or otherwise handles NPI [3] that is obtained when CU offers or delivers a financial product or service to an individual for personal, family, or household purposes, your org unit must comply with the GLBA Safeguards Rule. If your org unit accesses or maintains protected data (even if the unit does not have primary responsibility for offering the financial product or service), you must comply with the Safeguards Rule.

Examples of a financial product or service covered by the rule include:

- Any extension of credit by CU for household, personal, or family purposes (such as an extension of credit for tuition, fees, housing, or medical services).
- The provision or guarantee of loans under the Faculty Housing Assistance Program.
- The making or servicing of student loans or financial aid.

In these contexts, NPI must be safeguarded in all forms (not just electronic form), and in all org units with access to the data (e.g., via shared records systems) - whether or not the individual is ultimately extended credit or awarded financial aid.

While many org units will not conduct activities that subject the unit or program to the Rule’s specific requirements, it is important to be aware of the type of activities (financial products or services [9]) that may trigger future compliance requirements should your org unit operations change.

What must I do if my org unit is affected?

If your org unit handles or maintains covered data, your unit must follow CU's Data Governance [4] and Information Technology (IT) Security Program [5] policies and related guidance regarding the privacy and security of confidential and highly confidential information.

Additional steps your org unit should take:

- Review your internal policies and procedures to ensure that you have implemented appropriate administrative, technical, and physical safeguards [9] for NPI and other sensitive data.
- Train org unit employees about how to safeguard NPI to which they may have access in any form and ensure that they understand how to respond to and report [10] any potential intrusion or threat to CU information systems or data.
- Review any contracts with org unit service providers (see section below, *How are CU's service providers affected?*) that may collect or have access to NPI to ensure that adequate provisions to implement and maintain safeguards are in place.
- Contact your campus Office of Information Security for assistance is assessing potential risks to covered data and the adequacy of the safeguards your org unit may have implemented.

How are CU's service providers affected?

For purposes of the GLBA Safeguards Rule, a service provider is any person or entity that receives, maintains, processes, or otherwise is permitted access to NPI [3] through its direct provision of services to CU. CU must oversee service providers by taking reasonable steps to select and retain providers capable of maintaining appropriate safeguards for NPI -- and requiring them, by contract, to implement and maintain these safeguards.

Org units that collect, process, or otherwise handle NPI for university purposes with the assistance of external service providers must exercise due care in assessing the capabilities of these providers. The CU System Office of Information Security (OIS) has established IT purchasing standards [11] for this.

In addition, OIS (along with campus information security partners), provides assistance to units in conducting the necessary review. These offices, in collaboration with the Procurement Service Center and the Office of University Counsel, provide support to ensure service provider contracts include appropriate assurances regarding the safeguarding of sensitive personal information, including NPI, consistent with the requirements of the Rule and other applicable law.

Links
[1] https://www.cu.edu/controller/training/gramm-leach-bliley-act-glba-safeguards-rule
[2] https://www.ecfr.gov/cgi-bin/text-idx?node=pt16.1.314&rgn=div5
[3] https://www.cu.edu/controller/glba-safeguards-rule-examples-nonpublic-personal-information
[4] https://www.cu.edu/ope/aps/6010 [5] https://www.cu.edu/ope/aps/6005
[6] https://www.govinfo.gov/content/pkg/FR-2019-04-04/pdf/2019-04981.pdf
[7] https://www.cu.edu/regents/policy/8 [8] https://www.cu.edu/ope/aps/2027
[9] https://www.cu.edu/controller/glba-safeguards-rule-examples-financial-products-or-services
[10] https://www.cu.edu/security/reporting-incident [11] https://www.cu.edu/security/it-purchasing-standards-0