Gramm-Leach-Bliley Act

Guide to Safeguards Rule

April 26, 2023

Version 1.1

Contents

1 About This Document

Author UWSA IS Governance, Risk and Compliance Team

Change Authority UW System Office of Information Security

History

Version No.	Issue Date	Status	Reason for Change
1.0	04/20/2023	Published	Initial Publication
1.1	4/26/2023	Revised	Added scope section and other technical adjustments

2 Executive Summary

As a participant in Federal student financial aid programs (Title IV programs), institutions are required to comply with the Standards for Safeguarding Customer Information (Safeguards Rule), an important component of the Gramm-Leach-Bliley Act's (GLBA) requirements for protecting the privacy and personal information of customers (students).

On December 9, 2021, the Federal Trade Commission (FTC) issued an amendment to the Safeguards Rule, which was originally published in 2002, adding additional cybersecurity requirements and specific detail to existing requirements. Institutions are expected to coordinate with their leadership and appropriate staff to implement the new requirements by June 9, 2023.

Institutions are encouraged to:

1. Designate an individual at their institution, such as a SFA Director, to lead compliance efforts and coordinate with appropriate stakeholders to achieve compliance
2. Review this document and associated references to familiarize yourself with the detailed requirements of the rule
3. Complete a gap analysis/risk assessment of their current student information system landscape to gain an understanding what additional elements of the rule, if any, need to be undergone to achieve compliance. If resources are unavailable for this effort, strongly consider contracting with a third party to complete a Risk Assessment as discussed in section 3.2 below
4. Develop a plan to address identified gaps or areas of noncompliance
5. Document and monitor compliance with this Rule. While all elements are vital in protecting the security of student information, institutions may significantly reduce the risk of a security breach, and the resulting harm and inconvenience to its students, by encrypting student information while it is in transit outside its systems or stored on its systems and by implementing multi-factor authentication for anyone accessing student information on its systems

The remainder of this document serves as a resource and starting point to assist institutions in understanding the new Safeguards Rule requirements, explain the impacts of the changes on UW System, and describe changes to the Department of Education's (the Department) enforcement of GLBA requirements. Note that while this document provides a summary of the requirements, the best source of information is the text of the Safeguards Rule itself and GLBA guidance provided by the FTC.

2.1 Background

The Gramm-Leach-Bliley Act was developed by the FTC to require financial institutions to explain their information-sharing practices and safeguard sensitive data. Regarding the latter, the Safeguards Rule is the set of Cybersecurity requirements for the Gramm Leach Bliley Act. At its most basic level, the Safeguards Rule requires financial institutions to develop an information security program designed to protect customer information.

Postsecondary institutions must protect student financial aid information provided to them by the Department or otherwise obtained in support of the administration of the Title IV programs authorized under Title IV of the Higher Education Act of 1965. Each institution that participates in the Title IV programs has agreed in its Program Participation Agreement (PPA) to comply with the Safeguards Rule under 16. C.F.R. Part 314.

The original rule published in 2002 had three main components:

1. Designate an individual to coordinate the IS program
2. Perform risk assessments on select areas:
    - Employee training and management
    - Information systems (including network and software design), information processing, storage, transmission and disposal
    - detecting, preventing, and response capabilities
3. Document safeguards for each risk identified

The amended rule greatly expands on these original three requirements and adds additional requirements.

2.2 Scope

The Safeguards Rule uses the term "customer" and "customer information." For the purpose of an institution's compliance with GLBA, customer information is information obtained from the Department in support of applications for and receipt of Title IV student assistance, including financial data and PII.

In particular, the security requirements outlined in this document must be applied to all systems, databases, and processes that collect, process, and distribute customer information.

While the requirements of the Safeguards Rule are specifically applicable to information received from the Department, institutions are strongly encouraged to apply the requirements of the Safeguards Rule to *all* student data, especially since student data is combined in common systems and used by various departments and processes, regardless of the source of the information. In addition, many of the Safeguards Rule requirements are core security principles and requirements of the UW System Information Security Program and SYS 1000 Series: Information Security policy set.

2.3 Audience

This document is intended for information technology/security personnel and student financial aid staff responsible for administering student financial aid, protecting systems used in the course of such administration, and those responsible for protecting student data.

3 Requirements in the GLBA Safeguards Rule

Reflecting core data security principles, the objectives of the Safeguards Rule are to:

- Ensure the security and confidentiality of student information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any student.

To achieve these objectives, institutions are required to develop, implement, and maintain a written, comprehensive Information Security (IS) program. The IS program is required to contain administrative, technical, and physical safeguards that are appropriate to the size and complexity of the institution, the nature and scope of their activities, and the sensitivity of any student information.

The following nine elements must be included in the written IS program.

3.1 Designation of a Qualified Individual

Summary
Designate a 'qualified individual' responsible for overseeing and implementing the institution's IS program and enforcing the IS program.

Detail
The qualified individual must be someone who has the authority to review and approve alternative compensating controls and is required to report in writing, regularly and at least annually, to the board of directors or equivalent governing body on behalf of the institution.

The Qualified Individual may be an institutional employee, an affiliate, or a service provider. If the institution uses an affiliate or a service provider, the institution must:

1. Retains responsibility for compliance with the Safeguards Rule
2. Designate a senior member at the institution responsible for direction and oversight of the Qualified Individual; and
3. Require the service provider or affiliate to maintain an IS program that protects the institution in accordance with the requirements of the Safeguards Rule.

Recommendations
Formally designate a position to oversee the institution's IS program. Ideally, this should be the IS designee for each institution. This position should be captured within the enterprise IS program for each institution.

Reference: (16 C.F.R. 314.4(a))

3.2 Conduct Risk Assessment(s)

Summary
Risk assessment(s) shall be performed that identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of student information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.

Detail
The risk assessment shall be written and must include:

1. Criteria for the evaluation and categorization of identified security risks or threats you face;
2. Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and student information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and
3. Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the IS program will address your risks.

Additional risk assessments shall be performed periodically.

Recommendations
Develop a risk assessment approach to identify IT and operational processes and assess the levels of risk within each of the functional areas. The initial risk assessment shall be comprehensive and as such, we recommend this assessment is contracted out to a third party. The risk assessment should provide management visibility to process areas that contain the highest potential risk as determined by the IS risk assessment process. The following functional areas / processes within the institution should be considered for a comprehensive assessment:

Information System Domain/Process	Detailed Coverage of Functional Area / Process
Admissions	Student onboarding process, document storage, health information, transcript
Recruiting	Recruiting, marketing contact information, document storage
Marketing	Marketing contact information, information received from other departments and website for various campaigns
Registrar	Academic support, academic data, enrollment
Student Affairs	Student PII, health records, access to, processing, storage and sharing of data
Vendor Relationship	Administration, due diligence, contractual agreements, responsibility, and oversight third party relationships, SOC 2 Type 2 Reports
Student Financial Processing	Student financial aid, tuition, enrollment fees, student loan processing
Finance Department	Student account information, refund checks, tuition assessment, holds, collection process, student payroll
Human Resources	Access during the student hiring process

IT Domain/Process	Detailed Coverage of Functional Area / Process
Vulnerability Management	Review internal standards, procedures and results related to - authentication, patch management, configuration standards, malware protection, and intrusion detection and prevention
Independent/3rd Party Validation Processes	Review 3rd party procedures and results related to validation of - authentication, patch management, configuration standards, malware protection, intrusion detection and prevention, security architecture, network perimeter, vulnerability scanning, and penetration testing
Servers and Databases	Policy statements governing server data security, network shared drive review, local audit policy review, and password parameter review
Change Management	Project Administration, implementation & release, requirements gathering & analysis, end user training, program development, application / hardware changes, testing, emergency changes, data conversion and patch management
Organizational Administration	Organization structure, IS governance, policies, standards and procedures, risk management policy, maintenance, and storage of sensitive information (electronic and paper)
Electronic Information Processing	Web based applications, authentication standards, layered security, policies and procedures, password parameters, change management, administration
Logical Access	Application access, network access, and complexity standards
IS Personnel Administration	Hiring, training, rotation of duties, employee termination, contract resources
User Account Administration	Provisioning, de-provisioning, periodic validation, authentication, password management, segregation of duties
Application Administration	Internally and externally hosted and managed applications, access permissions, validation, application data, transaction process
Data Storage and Backup	Data storage types, backup schedule, inventory management, rotation, backup restoration
Workstation Administration	Authentication, configuration, anti-virus, privileges, encryption
Vendor Relationship	Administration, due diligence, contractual agreements, responsibility and oversight, third party relationships, SOC 2 Type 2 Reports
Physical Security and Environment Controls	Facility access, data center access, detective controls, environmental controls
Contingency Planning	Disaster recovery, incident response and business continuity, plan testing, responsibility, plan maintenance

Additional risk assessments shall be performed at a later date to assess if identified risks have been resolved and to identify any new risks that have appeared.

Reference: (16 C.F.R. 314.4(b))

3.3 Design and Implement Safeguards/Controls

Summary
Design and implement safeguards to control the risks the institution identifies through its risk assessment.

Detail
Safeguards should include:

1. ***Access controls***, including technical and, as appropriate, physical controls to:
    - Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of student information; and

- Limit authorized users' access only to student information that they need to perform their duties and functions, or, in the case of students, to access their own information;

2. ***Data classification and protection*** efforts to identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy. This includes:
    a. Develop, implement, and maintain procedures for the ***secure disposal*** of student information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the student to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and
    b. Periodically review your data retention policy to minimize the unnecessary retention of data;
3. ***Encrypt*** all student information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of student information, either in transit over external networks or at rest, is infeasible, you may instead secure such student information using effective alternative compensating controls reviewed and approved by your Qualified Individual;
4. Adopt ***secure development practices*** for in-house developed applications utilized by you for transmitting, accessing, or storing student information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store student information;
5. Implement ***multi-factor authentication*** for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;
6. Adopt procedures for ***change management***; and
7. Implement policies, procedures, and controls designed to ***monitor and log the activity*** of authorized users and detect unauthorized access or use of, or tampering with, student information by such users.

It is expected that future announcements by the Department will require compliance with NIST 800-171 as the Department views their data as Controlled Unclassified Information. Institutions are encouraged to begin familiarizing and adopting the IS controls required under NIST 800-171.

Recommendations
Ensure the controls identified above are implemented where appropriate.

Reference: (16 C.F.R. 314.4(c))

3.4 Test and Monitor Key Controls

Summary
Regularly test or otherwise monitor the effectiveness of the safeguards you have implemented.

Detail
Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:

1. Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and
2. Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your IS program.

Recommendations
Develop a testing and monitoring plan for key security controls. Identify systems within the scope of continuous monitoring and those without continuous monitoring, as described above.

For information systems without continuous monitoring, develop a plan for annual penetration testing. If penetration testing is performed annually, a different block or range of IP addresses can be tested and cycled year over year, however IP addresses tested should ultimately be influenced by the highest risk areas identified within the risk assessment.

Conduct vulnerability assessments every six months or sooner based on the conditions described in the detail above.

Reference: (16 C.F.R. 314.4(d))

3.5 Implement Policies and Procedures

Summary
Implement policies and procedures to ensure personnel are able to enact the IS program.

Detail
Policies and procedures shall address the following:

1. Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

2. Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the IS program;
3. Providing information security personnel with security updates and training sufficient to address relevant security risks; and
4. Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

Recommendation
Review and familiarize yourself with the enterprise IS policies and procedures, and supplement with institutional policies and procedures where appropriate. Institutional leadership should review bimonthly compliance reports detailing their compliance with UW System IS policies and provide adequate resources to address deficiencies.

Ensure staff receive and take security awareness training issued by UW Shared Services and provide training opportunities for staff to stay abreast of information security principles, best practices, and the threat landscape.

Reference: (16 C.F.R. 314.4(e))

3.6 Establish Oversight of Service Providers

Summary
Address how the institution will oversee its information system service providers.

Detail
Oversee service providers, by:
1. Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the student information at issue;
2. Requiring your service providers by contract to implement and maintain such safeguards; and
3. Periodically assess your service providers based on the risk they present and the continued adequacy of their safeguards.

Recommendation
Develop processes to assess and monitor the security practices of service providers. See the UW System Guide to Vendor Risk Assessments for more information.

Reference: (16 C.F.R. 314.4(f))

3.7 Keep Information Security Program Updated

Summary
Evaluate and adjust your IS program when appropriate

Detail
Evaluate and adjust the IS program in light of:

- the results of the required testing and monitoring;
- any material changes to operations or business arrangements;
- the results of the required risk assessments; or
- any other circumstances that may have a material impact on the IS program.

Recommendations
UWSA's Office of Information Security maintains the enterprise IS Program. This will be reviewed periodically and updated when necessary. The IS Designee/Qualified Individual should review and familiarize themselves with the IS Program.

Reference: (16 C.F.R. 314.4(g))

3.8 Establish an Incident Response Plan

Summary
A written incident response plan shall be maintained for institutions with 5,000 or more students.

Detail
The incident response plan shall address the following areas:

1. The goals of the incident response plan;
2. The internal processes for responding to a security event;
3. The definition of clear roles, responsibilities, and levels of decision-making authority;
4. External and internal communications and information sharing;
5. Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
6. Documentation and reporting regarding security events and related incident response activities; and
7. The evaluation and revision as necessary of the incident response plan following a security event.

Recommendation
UWSA's Office of Information Security has developed and maintains an enterprise incident response policy and plan. Institutions are encouraged to develop internal processes for responding to a security event that align with the enterprise incident response policy and plan.

Reference: (16 C.F.R. 314.4(h))

3.9 Reporting to the Board

Summary
Report, in writing, regularly and at least annually, to leadership on your overall status of compliance with the IS program and the Safeguards Rule. The report shall include material matters.

Detail
The Qualifying Individual is required to report in writing, regularly and at least annually, to the senior officer responsible for the IS program. If no such board exists, the reports shall be presented to a senior officer responsible for your IS program. The report shall include:

1. The overall status of the IS program and your compliance with the Safeguards Rule; and
2. Material matters related to the IS program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the IS program.

Recommendation
Develop a report that covers the detail listed above. This report shall be communicated by the IS Designee/Qualified Individual on an annual basis to the institution's chancellor as well as the UW System AVP for Information Security. The AVP for Information Security will summarize reports for all institutions and report to the Board of Regents on an annual basis to comply with this requirement.

Reference: (16 C.F.R. 314.4(i))

4 Audit, Enforcement, and Consequences for Noncompliance

It is expected that the Legislative Audit Bureau will complete audits on behalf of the Department to monitor compliance with the Title IV program.

If the Department determines that an institution is not in compliance with all of the Safeguards Rule requirements, the institution will need to develop and/or revise its IS program and provide the Department with a Corrective Action Plan (CAP) with timeframes for coming into compliance with the Safeguards Rule. Repeated non-compliance by an institution may result in an administrative action taken by the Department, which could impact the institution's participation in and ability to distribute financial aid through the Title IV program.

It is noted that the FTC recently created a special enforcement division that finds and prosecutes entities that have not complied with the Safeguards Rule.

APPENDIX A Definitions

Key definitions are included below. For a comprehensive list of definitions for 16 C.F.R. 314, see section 314.2 of the text.

Customer – Also referred to as student throughout this guide. Includes both past and present students or others you maintain a customer relationship with.

Customer (Information) – Information obtained from the Department as a result of providing a financial service to a customer (past or present).

Service Provider – Any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to the Safeguards Rule.

APPENDIX B Additional Resources

- 16 C.F.R. 314 – Standards for Safeguarding Customer Information
- Federal Student Aid Announcement – (GENERAL-23-09) Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements
- Protection Student Information – Compliance with CUI and GLBA
- FTC Safeguards Rule: What Your Business Needs to Know
- UWSA Office of Information Security's GRC Team
- NIST 800-171r2