Gramm-Leach-Bliley Act (GLBA) Training for the UW Community

November 2022
Office of the Chief Information Security Officer
Agenda

● GLBA: What is it?
  ○ Overview and definitions
● GLBA: What you need to know
  ○ Scope
  ○ Privacy Rule
  ○ Safeguards Rule
  ○ Compliance
● 2022 Update
● Questions
GLBA: What is it?
Gramm-Leach-Bliley Act (GLBA)

- Instituted in 1999
- Components:
  - Financial Privacy Rule 16 CFR 313
  - Safeguards Rule 16 CFR 314
- Applies to financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance
- Required to explain their information-sharing practices to their customers and to safeguard sensitive data
- Title IV/SAIG Institutions must protect Federal Student Aid (FSA) applicant information from unauthorized access/disclosure and comply with GLBA
GLBA Definitions

- Financial Institution - any institution engaging in financial activities.
  - As a Title IV institution, the University is subject to GLBA
- Customer - A customer relationship is a continuing relationship between a consumer and a financial institution providing a financial service.
- Consumer - One who obtains or has obtained a financial service but does not have an ongoing relationship with the institution.
Customer Information - any non-public personal information about a customer that is handled or maintained by or on behalf of the financial institution.

Examples of customer information include:

- Information provided to obtain a financial product or service;
- Information about a customer resulting from any transaction involving a financial product or service;
- Information otherwise obtained about a customer in connection with providing a financial product or service.
Non-Public Personal Information (NPI) - personally identifiable financial information that is:

- Provided by a consumer to a financial institution;
- Resulting from any transaction with the consumer or any service performed for the consumer; or
- Otherwise obtained by the financial institution.

Examples of NPI Include:

- Social Security Number (SSN)
- Financial account numbers
- Credit card numbers
- Date of Birth
- Name, address, and phone number
- Details of any financial transactions
GLBA: What You Need to Know
What you need to know

Because the University of Washington is subject to GLBA, you are required by law to safeguard personally identifiable financial information about students, parents, employees, and other “customers.”
GLBA Scope

Anything that processes, stores, or transmits NPI. For example:

- Servers, databases, and workstations
- Cloud-based services
- Network routers, switches
- Firewall and intrusion prevention system
- Safes, file cabinets, or desk drawers
- Shredding bins
GLBA Scope (cont.)

Financial services such as:

- Loans
  - Federal Family Education Loan (FFEL)
  - Direct Loan
  - Federal Perkins Loan
  - Institutional Loans
- Grants
  - Federal Pell Grant
  - Federal Supplemental Educational Opportunity Grant (FSEOG)
- Federal Work-Study (FWS) Program
GLBA Scope (cont.)

The University uses third-party service providers for collections, payment plans, loan processing, etc.

**You cannot outsource compliance responsibility.**

Work with UW Procurement to ensure all GLBA due diligence and required contract language are addressed.
GLBA Scope (cont.)

Non-public personal information that a consumer provides to obtain a financial service/product:

- FAFSA and Application Data
  - Supporting documentation such as tax returns
- Any NPI stored, transmitted, or processed as part of GLBA covered services
  - Social security numbers
  - Financial statements/balances
  - Loan applications
  - Credit history
  - Account numbers
Protected from what?

- Unauthorized disclosures
- Overheard sensitive conversations
- Information on paper
- Inappropriate access
- Insecure storage
- Comingling of student records

- Ransomware
- Virus/Malware
- System misconfiguration
- Failed/missed software patches
- Malicious Internet sites
- Email phishing
Privacy Rule

- Written notice describing privacy policy and practices (including sharing with 3rd parties).
- Written notice describing how customer (and former customer) NPI is collected, disclosed, and protected.
- Notice must provide an accurate description of current practices and policies to ensure confidentiality and security of customer NPI.
- Notice must provide an opportunity for customers to opt-out of sharing with non-affiliated 3rd parties.

The FTC has officially stated that any college or university that complies with the Federal Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) and that is also a financial institution subject to the requirements of GLBA shall be deemed to be in compliance with GLBA’s privacy rules if it is in compliance with FERPA (16 CFR 313.1).

Consult with the UW Privacy Office for guidance on addressing the Privacy Rule.
Safeguards Rule

The Safeguards Rule requires all financial institutions to:

- Develop, implement, and maintain a written information security program
- Designate a single Qualified Individual to oversee the information security program
- Identify and assess risks
- Provide appropriate service provider oversight
- Periodically evaluate and update the security program based on identified risks
Safeguards Rule Compliance

Designate the Qualified Individual responsible for overseeing and implementing the information security program

- Responsible for program implementation
- Identify and assess risks
- Verify third-parties are capable of maintaining safeguards
- Ensure the program is reviewed annually and updated as needed
- Must be qualified to perform the role (2022 update)
- Report in writing at least annually to the institution’s governing body
Safeguards Rule Compliance

Identify and Assess Risks

- Periodic risk assessments
- Assign risk ratings based on likelihood of impact and occurrence
- Focused on risks to covered information
- Must identify at least one risk for each of the following areas:
  - 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 system failures
- Perform additional risk assessments to regularly review specific identified risks (2022 update)
Safeguards Rule Compliance

Design and Implement Safeguards

- Design and implement safeguards to address identified risks
- Regularly test and monitor the effectiveness of key controls
- Monitor system activity for unauthorized use of customer information (2022 update)
- Encrypt customer information both in transit and at rest (2022 update)
- An auditor will verify that the institution has implemented safeguards for identified risks
GLBA Non-Compliance

- The institution shall be subject to a civil penalty up to $100,000 for each violation.
- Officers shall be personally liable for civil penalties not more than $10,000 for each violation.
GLBA: 2022 Update
GLBA 2022 Update

FTC updated the GLBA Safeguards Rule effective December 9, 2021 with several requirements subject to a one year delay.

Key provisions:

- Written risk assessments
- Enhanced personnel qualification and training requirements
- Oversight of service providers including periodic compliance assessment
- “Security Event” definition broadened and specifically extended to paper or “hard copy” records
GLBA 2022 Update (cont.)

Addition of specific controls

- Multi-factor authentication
- Physical access controls
- Requiring access model to follow the “Principle of Least Privilege”
- Encryption of data both in transit and at rest
- Inventory of assets (data, systems, facilities, etc.)
- Secure development practices
- Change management
- Logging and system monitoring
- Regular penetration testing and vulnerability assessment
- Written incident response plan
- Secure disposal of information within two years of last use

Note: The Department of Education has not yet issued guidance or audit objectives for the new GLBA requirements.
The Bottom Line

Have a sound security plan in place to:

- Collect only what you need
- Keep it safe
- Dispose of it securely

- Federal Trade Commission
Resources

Federal Trade Commission - GLBA

Federal Trade Commission - Identity Theft
www.identitytheft.gov

UW CISO - education
https://ciso.uw.edu/education/

UW Contract Terms & Conditions
https://finance.uw.edu/ps/suppliers/terms-conditions

UW Administrative Policy Statements 2.2, 2.3, 2.4, 2.5, and 2.6:
https://www.washington.edu/admin/rules/policies/APS/TOC00.html
Questions?

ciso@uw.edu