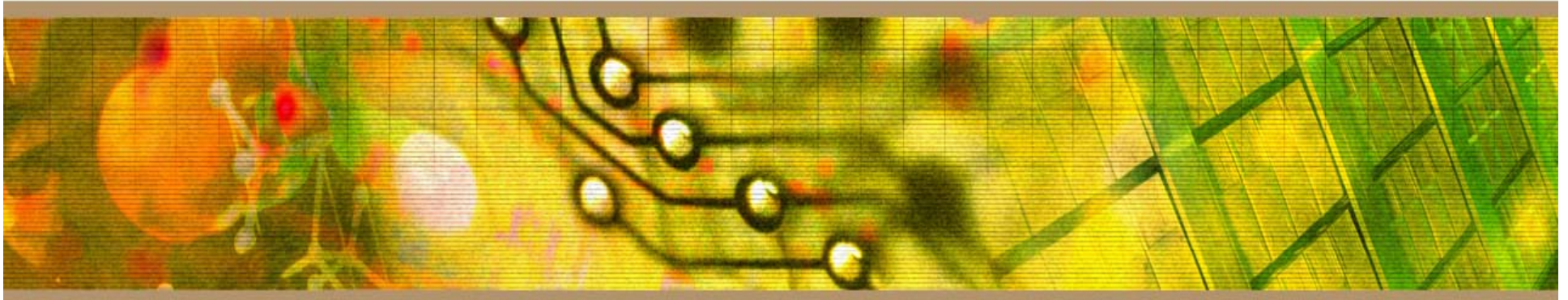




# Gramm Leach Bliley Act 15 U.S.C. §§ 6801-6809



GLBA/HIPAA Information Security Program Committee  
GLBA, Safeguards Rule Training, Rev. 7/1/2007



- GLBA Overview
- Safeguards Rule
- Additional Resources
- GLBA Definitions

- The Gramm Leach Bliley Act (GLBA) is a comprehensive, federal law affecting financial institutions. The law requires financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of customer information.
- The Federal Trade Commission (FTC) enforces compliance with GLBA.
- The FTC may bring an administrative enforcement action against any financial institution for non-compliance with the GLBA.

- Purdue University significantly engages in student loan making and provides other financial services to student customers. As such, Purdue falls within the definition of “financial institution” under the GLBA and must comply with the law’s requirements.
- “Financial Institution” means any institution the business of which is engaging in financial activities.

- Examples of Purdue University Financial Products and Services Covered Under GLBA:
  - Student loans, including receiving application information, and the making and servicing of such loans
  - Financial advisory services (very limited at Purdue)
  - Collection of delinquent loans
  - Check cashing services
  - Tax planning (very limited at Purdue)
  - Obtaining information from a consumer report
  - Career counseling services for those seeking employment in finance, accounting or auditing

- The GLBA is composed of several parts, including:
  - the Privacy Rule (16 CFR 313) and
  - the Safeguards Rule (16 CFR 314).

- The FTC has officially stated that any college or university that complies with the Family 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).

- The FTC has not made a similar exception for an institution of higher education with respect to the Safeguards Rule.
- The Safeguards Rule requires all financial institutions to develop an information security program designed to protect “customer information.”
- Purdue University must comply with the Safeguards Rule.

- The objectives of the Safeguards Rule are to:
  - Insure the security and confidentiality of customer 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 customer.

- “*Information Security Program*” means the administrative, technical, or physical safeguards used by a financial institution to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.
- Under Purdue’s Information Security Program, a GLBA-covered department must assume responsibility for assuring adequate safeguards are in place within its area of responsibility.

- The Information Security Program must include:
  - Designation of staff to coordinate the safeguards program
  - Identification and assessment of risks in each relevant area of the operation and an evaluation of the effectiveness of current safeguards
  - Design and implementation of a safeguards program including regular monitoring and follow-up
  - Selection of appropriate service providers including inclusion of contract language designed to protect customer information handled by third party service providers
  - Evaluation and adjustment of the program in light of relevant circumstances and changes in business.

- There are three types of safeguards that must be considered when a Purdue department implements safeguards to protect the security, confidentiality, and integrity of customer information :
  - Administrative Safeguards
  - Technical Safeguards
  - Physical Safeguards

- *Administrative Safeguards* include developing and publishing policies, standards, procedures, and guidelines, and are generally within the direct control of a department. Examples include :
  - Reference checks for potential employees
  - Confidentiality agreements that include standards for handling customer information
  - Training employees on basic steps they must take to protect customer information (see detail later slide)
  - Assure employees are knowledgeable about applicable policies and expectations
  - Limit access to customer information to employees who have a business need to see it
  - Impose disciplinary measures where appropriate

- *Physical Safeguards* are generally within a department's control and include:
  - Locking rooms and file cabinets where customer information is kept
  - Using password activated screensavers
  - Using strong passwords
  - Changing passwords periodically and not writing them down
  - Encrypting sensitive customer information in transit and at rest
  - Referring calls or requests for customer information to staff trained to respond to such requests
  - Being alert to fraudulent attempts to obtain customer information and reporting these to management for referral to appropriate law enforcement agencies

- Physical Safeguards also include:
  - Ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods
  - Store records in a secure area and limit access to authorized employees
  - Dispose of customer information appropriately:
    - » Designate a trained staff member to supervise the disposal of records containing customer personal information
    - » Shred or recycle customer information recorded on paper and store it in a secure area until the confidential recycling service picks it up
    - » Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contains customer information
    - » Promptly dispose of outdated customer information according to record retention policies

- *Technical Safeguards* include the configuration of computing infrastructure and are generally the responsibility of centralized or departmental/zone IT computing staff. Departments should be knowledgeable regarding how their digital customer information is safeguarded. If additional technical controls are warranted, departments should work with IT staff to improve safeguards.
- Departments are also responsible for alerting IT staff to the existence of customer information on networks

- Technical safeguards include:
  - Storing electronic customer information on a secure server that is accessible only with a password - or has other security protections - and is kept in a physically-secure area
  - Avoiding storage of customer information on machines with an Internet connection
  - Maintaining secure backup media and securing archived data
  - Using anti-virus software that updates automatically
  - Obtaining and installing patches that resolve software vulnerabilities
  - Following written contingency plans to address breaches of safeguards
  - Maintaining up-to-date firewalls particularly if the institution uses broadband Internet access or allows staff to connect to the network from home
  - Providing central management of security tools and keep employees informed of security risks and breaches

- In addition to developing their own safeguards, financial institutions are responsible for taking steps to ensure that their affiliates and service providers safeguard the customer information in their care.
- “*Affiliate*” means any company that controls, is controlled by, or is under common control with another company.
- “*Service Provider*” means any person or entity that receives, maintains, processes, or otherwise is permitted to access customer information through its provision of services directly to a financial institution.

- Purdue University uses the PUID as a unique identifier in many business transactions.
- The PUID is classified as “sensitive” University data and must be protected as such under the data handling guidelines.
- Information about the PUID is available at:
  - <http://www.purdue.edu/securepurdue/puid/Welcome.cfm>

- GLBA/HIPAA Information Security Program Committee
  - <http://www.purdue.edu/securepurdue/securityPrograms.cfm>
- Many of Purdue's existing IT policies address some of the compliance issues raised in the GLBA Safeguards Rule.
  - [http://www.purdue.edu/policies/pages/information\\_technology/info\\_tech.html](http://www.purdue.edu/policies/pages/information_technology/info_tech.html)
- Purdue Social Security Number policy
  - [http://www.purdue.edu/policies/pages/information\\_technology/v\\_5\\_1.html](http://www.purdue.edu/policies/pages/information_technology/v_5_1.html)
- All Purdue policies
  - <http://www.purdue.edu/policies/>

- SecurePurdue website for links to information security policies, standards, and best practices.
  - <http://www.purdue.edu/securepurdue/bestPractices/>
- SecurePurdue website for links on identity theft and identity protection.
  - <http://www.purdue.edu/securePurdue/theft.cfm>
- University Data Handling Classifications and Guidelines.
  - <http://www.purdue.edu/securepurdue/bestPractices/dataClass.cfm>

- Additional guidance regarding GLBA is available at:
  - <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

- Additional Questions?
  - Contact your manager for specific procedural questions in your area.
  - Contact IT Networks and Security for information regarding risk assessments, educational materials, and questions about computer security at [itap-securityhelp@purdue.edu](mailto:itap-securityhelp@purdue.edu)
  - Contact Purdue's Chief Information Security Officer for questions about the GLBA/HIPAA Program Committee.

# GLBA Definitions

- *Customer Information* is any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates.

- GLBA applies to customer information obtained in a variety of situations, including:
  - Information provided to obtain a financial product or service;
  - Information about a customer resulting from any transaction involving a financial product or service between the institution and a customer;
  - Information otherwise obtained about a customer in connection with providing a financial product or service to the customer.

- *Non-Public Personal Information* means 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.
- The term also includes 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.

- Examples of Non-public Personal Information (NPI) Include:
  - Social Security Number (SSN)
  - Financial account numbers
  - Credit card numbers
  - Date of birth
  - Name, address, and phone numbers when collected with Financial data
  - Details of any financial transactions