

CYBER SECURITY

Newsletter

GLBA FOR SCHOOLS

Problem

The Gramm Leach Bliley Act was passed by Congress in 1999 and is enforced by the Federal Trade Commission. This act, also known as GLBA, is a federal law that protects customer's non-public personal information, otherwise known as NPI. NPI is any personally identifiable financial information a customer provides to obtain a financial service or product. Examples of NPI include social security numbers, credit card numbers, account balances, tax return information, driver's license numbers, and dates of birth.

GLBA dictates several specific requirements and is comprised of two categories: the Financial Privacy Rule and the Safeguards Rule. Colleges and universities are deemed to be in compliance with the Financial Privacy Rule of GLBA if they are in compliance with the Family Educational Right and Privacy Act, commonly known as FERPA.

However, higher education institutions are subject to the Safeguards Rule Act related to the administrative, technical, and physical safeguarding of consumer information. The purpose of this rule is to ensure our school is protecting our students. As a result, whenever you are handling any NPI you must adhere to the following rules, regardless if the data is in physical, digital or oral format.

- Use only authorized systems to enter, process or store NPI. Do not copy or store NPI to unauthorized systems.
- Do not use NPI systems for non-work related or unauthorized activities, such as surfing personal websites, reading personal email or chatting with someone online. Activities such as these can expose customer data to great risks.



GLBA ACT

The Gramm Leach Bliley Act is a federal act that schools must adhere to. Specifically, the protection of non-public personal information or NPI. In this newsletter we describe what NPI is and how we must protect it.

JUNIATA
COLLEGE 

This newsletter is published by
Campus Technology Services. For
more information please contact
us at:
help@juniata.edu

Why GLBA Applies to Our School

GLBA protects "any individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family or household purposes, and also means the legal representatives of such an individual." (See 15.U.S.C. § 6809(9)).

You may think it is odd for our school to be considered as a financial institution, but remember we provide an extensive amount of financial services, such as helping students with student loans. This requires us by Federal law to ensure the safeguarding of any NPI.

- Limit access to customer information to only authorized personnel who have a business need to see it.
- Transfer of NPI must use secure, authorized methods, including the use of encryption. Do not transfer NPI using insecure means such as email unless sensitive data has first been encrypted.
- Any NPI related information must be protected by strong passwords.
- If you collect information online directly from customers, make sure the transmission is automated. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.
- Refer calls or other requests for customer information to designated individuals who have been trained in how your institution safeguards personal data.
- Use password-activated screen savers to lock computers after a period of inactivity.
- Store NPI records in a room or cabinet that is locked when unattended.
- All physical and electronic NPI that is no longer necessary or appropriate to store must be properly destroyed, shredded or rendered unreadable.
- Immediately report any lost or stolen NPI to your help desk or information security team.

By following these steps, you ensure our organization is not only secure but compliant. If you have any questions about what NPI is, or how to best secure it, please contact your IT help desk or information security team.