JOSEPH F. McCLOSKEY SCHOOL OF NURSING

Gramm-Leach-Bliley Information Security Program

Overview

The School of Nursing (SON) takes seriously its responsibility to safeguard personal data and its obligation to comply with the various federal, state and international laws related to the protection of personal, sensitive or otherwise protected data for which it collects. One of these laws, the Gramm-Leach-Bliley Act ("GLBA") requires that the School of Nursing implement an information security program designed to protect and safeguard all non-public information (NPI) which it has collected for the purpose of offering a financial product or service.

Purpose

(1) insure the security and confidentiality of covered information; (2) protect against anticipated threats or hazards to the security and integrity of such information; and (3) protect against unauthorized access or use of such information that could result in substantial harm or inconvenience to customers.

Applicability of the Procedure

This policy applies to all SON staff, faculty, LVHN staff, and third parties who have access to student financial data and who require the ability to access, use or disclose NPI as part of their job duties.

Definitions

Customer:	means any individual who receives a financial product or service from the SON. Most often it will be a student or their parent(s)/legal guardian(s). It could also include spouses, faculty, staff or other third parties.
Gramm-Leach Bliley Act (GLBA)	is also known as the Financial Services Modernization Act of 1999. GLBA is a federal law that requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. Through its lending programs, the School of Nursing is required to comply with GLBA for those areas of its operations related to this lending.
Non-Public Personal Information (NPI)	is personally identifiable information (PII, defined below) which is (1) provided by a customer to the School of Nursing, (2) provided by another financial institution to the School of Nursing, or (3) otherwise obtained by the School of Nursing for the purpose of offering a financial product or service. Example of NPI include, but are not limited to: • Financial Account Numbers (bank, credit card) • Credit Rating/Credit Data • Social Security Numbers • Loan Documents/Payoff Amounts • Tax Returns • Asset Statements

Personally Identifiable Information (PII) is information that can be used by itself or in combination with other information to identify an individual.

Examples of PII include, but are not limited to:

- Name
- Physical Address
- Email Address
- Date of Birth
- Mother's Maiden Name
- Phone Number
- Social Media Account Name

Procedure

GLBA requires that the GLBA Information Security Program include the following elements. The School of Nursing's procedures as they relate to these elements are as follows:

1. *Designate one or more employees to coordinate its GLBA information security program.* The Director IS Security is the individual responsible for coordinating its GLBA information security program. The Director, SON, has been designated as the individual with day-to-day oversight of the program.

2. *Identify and assess the risks to customer information as it relates to the School of Nursing's provision of financial products or services; 3. Evaluate the effectiveness of the current safeguards for controlling these risks; 4. Design and implement a safeguards program, and regularly monitor and test it.*

   The Director IS Security will work with the Director, SON to identify risks to security and privacy of the SON's financially related information systems. While the Director IS Security is primarily responsible for internal and external risk assessment of LVHN systems including those that store NPI, all members of the LVHN and SON that deal with the SON's NPI and PII are responsible for safeguarding NPI.

   The Director IS Security, in consultation with the Director, SON, will conduct regular data security reviews of the SON's financially related information systems and services. The Director IS Security will perform an annual risk assessment related to the handling of NPI that will include documentation of internal controls. Management remains responsible for the review and identification other security risks, including the storage of paper records or other records that contain NPI data. The Director, SON is responsible for ensuring that the SON information, including NPI, within the area of assigned responsibility is used with appropriate, controlled levels of access and with assurance of its confidentiality and integrity. The Director IS Security is available to provide guidance to management during this process.

   Access to the SON financially related information systems and services is provided on an as-needed basis. Access is requested by the individual user's supervisor and approved by the Director, SON.

The Director IS Security, in coordination with the Director, SON, is responsible for assuring physical security of the SON's primary system that houses HPI, as well as of the network that the SON uses to access this system. During risk assessments of other LVHN areas, the Director IS Security will notify the Director, SON of other systems identified that contain NPI related to GLBA. As identified, the Director IS Security and Director, SON will work together to develop a mitigation plan for any risks associated with those identified systems.

5. Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information.

As part of the LVHN procurement process, those contracts for technology that require access to NPI will undergo a security review.

6. Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

Policies are reviewed every three years unless otherwise specified. In addition to the regularly scheduled reviews, through LVHN's Information Security Procedures, LVHN requires that the Director IS Security and Director, SON, update the Policy as legal requirements and best practices evolve, in addition, as part of the risk management program, risks are reviewed and mitigation plans developed using a risk-based approach.

Inquiries

All correspondence and inquiries should be directed to Richard Fronheiser, Director IS Security at Richard.Fronheiser@lvhn.org

JOSEPH F. McCLOSKEY SCHOOL OF NURSING
Frequently Considered Areas for Gramm-Leach-Bliley Covered Data

Area	Type of Information
Director, School of Nursing	Student aid eligibility, Student and parent financial data, credit card, banking, and registration data
Admissions Coordinator/Financial Aid Administrator	Student aid eligibility, Student and parent financial data
Bursar	Student and parent financial data; credit card, banking, and registration data
Registrar	Student financial and banking/credit card data, and student records
LVHN finance	Credit card, banking, and registration data, student and parent financial data
LVHN Accounts payable	Credit card, banking, and registration data, student and parent financial data
LVHN Human Resources/Payroll	Employee benefits, personal deduction, retirement contribution and banking information
LVHN Compliance	Student and Employee financial data

LVHN Technology Department	Administration of central information systems for Human Resources, financial and student records. Administration of network, PC and office system services that are used by SON offices listed herein to process, transmit, and store covered data.
LVHN Health Services	Student records