Information Security and Legal Compliance

Module 12

Simplifying Security.

Certified Secure Computer User

Module 12: Information Security and Legal Compliance

Exam 112-12

Module Objectives

In order to ensure **confidentiality of information**, laws were passed such as the Health Insurance Portability and Accountability Act (**HIPPA**), Family Educational Rights and Privacy Act (**FERPA**), and Payment Card Industry Data Security Standard (**PCI DSS**) to regulate information security. These laws impose obligations on colleges and universities to protect the data they collect, process, store, use, and disclose. Risk assessment and mitigation value is likely higher in **compliance** with information security policies, standards, and procedures. Failure to protect the data by colleges and universities will result in public embarrassment and **penalties** associated with managing the response to incidents.

This module will familiarize you with the:

- HIPPA (Health Insurance Portability and Accountability Act)
- HIPPA Checklist
- FERPA (Family Educational Rights and Privacy Act)
- FERPA Checklist
- PCI DSS (Payment Card Industry Data Security Standard)
- PCI DSS Checklist

Module Flow

Health Insurance Portability and Accountability Act (HIPPA)

Family Educational Rights and Privacy Act (FERPA)

Payment Card Industry Data Security Standard (PCI DSS)

HIPPA

The Health Insurance Portability and Accountability Act were enforced in 1996. It was mostly created to provide **protection for personal health information**. HIPPA legislation was created by the secretary of Health and Human Services (HHS).

HIPPA is a security standard to provide **physical**, **technical**, and **administrative safeguards** to **protect** the integrity, availability, and confidentiality of health information. The purpose of this security standard is to prevent the **inappropriate use** and **disclosure** of an individual's health information. It imposes restrictions on organizations to protect health information and the systems that store, transmit, and process it.

Objectives of HIPPA include:

- Group and individual insurance reform
- It allows for the portability and continuity of health insurance and places limits on pre-existing exclusion provisions
- It reduces the potential for waste, fraud, and abuse
- New penalties and sanctions will be imposed
- It requires the application of uniform standards to electronic data transactions in a confidential and secure environment
- Its goal is to improve the effectiveness and efficiency of the health-care system

HIPPA Checklist

File Security

- File cabinets or drawers that store patient records should be **securely locked**, or if possible, the room itself.
- **Restrict access** to computer terminals to only authorized personnel and set up passcodes for electronic files.
- Be aware of the security lapses that might allow illegitimate users access to the records.

Education and Sanctions

- A professional workforce should be **trained** with HIPPA requirements, both on and off the job
- Ensure that the employees know about the **repercussions** of violating HIPPA restrictions.
- Violators of HIPPA are punished to send a message to the other employees that HIPPA is a **serious consideration** within the organization

Authorization Procedures

- Ensure that only authorized personnel have **access** to HIPPA-protected information.

- **Review the file logs** or computer records regularly to know how the authorization is used to ensure that it is not abused.

FERPA

The Family Education Rights and Privacy Act (FERPA) of 1974, also known as the **Buckley Amendment**, is a federal law that is meant to **protect the accuracy** and **privacy** of **student education records**. This law is applicable to all institutions that are recipients of federal aid directed by the Secretary of Education. FERPA gives certain rights to parents with respect to their children's educational records. These rights transfer to the student when he/she reaches the age of 18 or a school beyond the high-school level.

The rights given to the students regarding the educational records by FERPA include the:

- **Right to access** educational records kept by the school
- **Right to demand** educational records be disclosed only with student permission
- **Right to amend** educational records
- **Right to file complaints** against the school for disclosing educational records that violate FERPA
- **Right to know** about the purpose, content, and location of information kept as a part of their educational records

Individual staff or faculty's private notes, campus police records, medical records, and statistical data compilations that do not contain personally identifiable student information are not considered educational records under FERPA.

FERPA Checklist

- Post grades using **secure technology**.
- Ensure that the confidential, non-directory, and sensitive student personal information is **encrypted** on whatever it is stored, including laptops and thumb drives.
- Do not use social security numbers for any purpose unless necessary. Replace them with **universal identification numbers** (UINs).
- Do not leave graded tests or papers in a stack for students to pick up by sorting through them.
- Do not provide anyone with student schedules or assist anyone other than professional university employees in finding a student on campus.
- Do not link the name of a student with his or her social security number or UIN in any public manner.

- Do not discuss the progress of any student with anyone other than the student (including parents/guardians) without the consent of the student.
- Do not provide anyone with lists of students enrolled in classes for any commercial purpose.
- Institutions must have **written permission** from the student to release any information from a student's educational record.
- Only student directory information can be disclosed by the institutions without the student's permission, but not non-directory information.
- Students should be notified about their rights under FERPA by institutions through annual publications.

PCI DSS

PCI DSS is a worldwide information security standard defined by the **Payment Card Industry Security Standards Council**. PCI DSS is a set of guidelines, measures, and controls that were established to assist merchants implement **strong security** precautions to ensure **safe credit card usage** and **secure information** storage.

This was created by four major credit cards companies in 2004: Visa, MasterCard, Discover, and American Express. Businesses with merchant identification that takes credit card payments—whether online, over the phone, or using credit card machines or paper forms—need to comply with these standards, even if they use a payment service provider.

PCI DSS objectives include:

- Maintain an information security policy
- Build and maintain a secure network
- Regularly monitor and test networks
- Protect cardholder data
- Implement strong access control measures
- Maintain a vulnerability management program

PCI DSS Checklist

The 12 major points in the checklists that is created by PCI SSC include:

- Install and maintain a **firewall** configuration to protect cardholder data.
- **Restrict access** to cardholder data to need-to-know.
- Protect stored cardholder data.

- Assign a unique ID to each person with computer access.
- Do not use vendor-supplied **defaults** for system **passwords** and other security parameters.
- **Restrict** physical **access** to cardholder data.
- **Encrypt** the transmission of cardholder data across open, public networks.
- Track and monitor all access to network resources and cardholder data.
- Use and regularly **update anti-virus** software.
- Regularly **test security systems** and processes.
- Develop and maintain secure systems and applications.
- Maintain a policy that addresses information security.

Module Summary

HIPPA is a security standard to provide physical, technical, and administrative safeguards to protect the integrity, availability, and confidentiality of health information.

HIPPA is intended to prevent the inappropriate use and disclosure of individuals' health information.

FERPA is a federal law that is meant to protect the accuracy and privacy of student education records.

PCI DSS is a set of guidelines, measures, and controls that were established to assist merchants implement strong security precautions to ensure safe credit card usage and secure information storage.

Businesses with merchant identification that accepts credit card payments—whether online, over the phone, or using credit card machines or paper forms—need to comply with PCI DSS standards.