Policy Title	Original Adoption Date	Policy Number
Protection of Sensitive Information	01/19/2015	IN-710
Responsible College Division/Department	**Responsible College Manager Title**	
Technology	Vice President of Administrative Services	

Policy Statement

I. PURPOSE & APPLICABILITY

The purpose of this Policy is to help protect the confidentiality and integrity of sensitive information. This Policy requires the protection of sensitive information including Personally Identifiable Information (PII), Payment Cardholder Information (PCI), other types of financial account/payment information, Protected Health Information (PHI), competitive business information, and non-directory Family Educational Rights and Privacy Act of 1974 (FERPA) information. This Policy applies to all employees.

II. REQUIREMENTS

Sensitive information should only be collected, used, shared, transmitted, and stored when there is an academic, financial, patient care, community relations, or business purpose. Sensitive information shall not be posted to web sites, portal sites, unprotected shared drives, or any other location that compromises the confidentiality or integrity of the information. All sensitive information shared with vendors must be pre-approved by the Data Governance Committee. This includes information stored at vendor facilities or in the cloud.

All electronically transmitted and stored sensitive information must be encrypted including information on portable storage devices like USB drives. An exception to encryption may be requested, which will be reviewed and approved by the Data Governance Committee. Paper documents containing sensitive information must be kept under control at all times, transferred internally via sealed envelope, and stored in a locked container. Any employee that suspects sensitive information has been lost, compromised, or disclosed without authorization must be immediately notify the Director of Technology. Sensitive information must be retained according to the appropriate record retention policy or, if allowed per the policy, destroyed. Sensitive information must be destroyed via shredding if on paper, permanently deleted if stored electronically, or the physical media must be destroyed if stored electronically and permanent deletion is not possible.

The President, Vice Presidents, Deans, Directors, and Managers have ultimate accountability for compliance with this Policy in their division/department, even if specific responsibilities are delegated. They must ensure employees in their area of responsibility are aware of and comply with this Policy. They are responsible for ensuring their division/department maintains an inventory of its stored sensitive information and must provide the inventory list to the Director of Technology upon request. They must also review all requests for an exception to encryption within their division/department and, if they concur with the request, they should forward the request to the Data Governance Committee.

The Director of Technology is responsible for developing, implementing, updating, and enforcing this Policy. The Director will also periodically review division/department sensitive information inventories and take immediate action upon the report of sensitive information that has been lost, compromised, or disclosed without authorization.

The Data Governance Committee is responsible for approving requests to share sensitive data with vendors and that the vendor provides sufficient information on their ability to safeguard LTC sensitive information. The Committee will also review and approve/deny requests for encryption exceptions.

Reason for Policy

LTC is committed to protect sensitive information that is in its custody or control.

Historical Data, Cross References and Legal Review

Created/Adopted: 01/19/15
Reviewed/Revised: 05/21/19
Cross References: Wis.Stat.134.98(1)(b), Federal Regulations Title 34 §a Part 99, LTC Vendor security agreement
Legal Counsel Review and Approval:
Board Policy: III.F. Asset Protection

Definitions

Personally Identifiable Information (PII) means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:

1. The individual's social security number.
2. The individual's driver's license number or state identification number.
3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.
4. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

Payment Cardholder Information (PCI) means debit/credit card numbers, expiration dates, track 1/2 data, etc.

Other Types Of Financial Account/Payment Information means bank/brokerage account numbers, ACH codes, balances, debts, etc.

Protected Health Information (PHI) means health records, treatment data, etc.

Competitive Business Information means intellectual property, legal/compliance, or other types of data elements subject to client-assigned confidentiality requirements.

Non-Directory Family Educational Rights and Privacy Act of 1974 (FERPA) Information means information contained in the education records of a student that would be considered harmful or an invasion of privacy if disclosed. Non-directory information includes all information in a student record *except* student identification number, name, address, telephone listing, date and place of birth, campus email, participation in officially recognized activities and sports, and dates of attendance including program and degree earned.