Policy Title	Original Adoption Date	Policy Number
Protection of Electronically Stored Personal Information	01/19/2015	IN-710
Responsible College Division/Department	**Responsible College Manager Title**	
Information Technology Services	Director of Information Technology	

Policy Statement

I. PURPOSE & APPLICABILITY

The purpose of this Policy is to:

1. Require encryption of electronically stored Personal Information;
2. Assign responsibility for compliance; and
3. Establish the authority and procedures to request exceptions to encrypting electronically stored Personal Information.

This Policy requires the encryption of electronically stored Personal Information, thereby minimizing the risk of a breach. However, should a breach occur, the College has formal procedures to minimize and mitigate the impact of such an incident. This Policy serves to identify and protect electronically stored Personal Information.

This Policy applies to:

- Division/Department Heads
- Data Stewards

II. STATEMENT

Personal Information in the custody or control of LTC should be stored only when there is an academic, patient care, community relations or business purpose for doing so.

All electronically stored Personal Information must be encrypted, including backups. Personal information must not be stored on a mobile device (see Definitions), even if the device and/or the data is encrypted.

Each division/department must maintain an inventory of its electronically stored Personal Information, if applicable, including individuals responsible for this Personal Information.

Division/Department Heads have the authority to impose more restrictive standards for electronically storing Personal Information in their area of responsibility.

Employees who violate this Policy will be subject to the disciplinary process in accordance with College policies.

Exceptions to Encryption of Electronically Stored Personal Information

An exception to encryption may be requested only if the Personal Information cannot be encrypted or there are circumstances that make it inappropriate to do so (e.g. system or application performance).

Requests for an exception must be reviewed and approved by the Information Security Officer on a case-by-case basis.

Other Relevant Policies, Requirements and Offices

Various LTC offices have responsibility for the oversight of, or regulatory compliance with requirements for the privacy and security of certain types of data that overlap with Personal Information. These include, but are not limited to, the following:

1. Medical records
2. Credit card data under the responsibility of Financial Services and Student Services.
3. Background check information under the responsibility of Human Resources and Student Services.
4. As it pertains to contracts that are established with third-parties - contractors, consultants, or external vendors - working with Personal Information must include satisfactory assurances that the contracting third-party will appropriately safeguard College information; and
5. LTC policy Minimum Security Standards for Network Devices - devices connecting to the LTC network, including those storing Personal Information, must comply with the security standards set forth in that policy.

IV. RESPONSIBILITIES

Specific responsibilities and duties are assigned in order to implement and ensure compliance with this Policy. In addition, there are designated College officials who are assigned the responsibility to review requests for exception to encryption and to approve, or recommend approval of such requests.

Division/Department Heads have ultimate accountability for compliance with this Policy in their organization, even if specific responsibilities are delegated. Each Division/Department Head must:

1. Ensure that Data Stewards in their area of responsibility are aware of and comply with this Policy;
2. Review all requests for an exception to encryption within their division/department and recommend whether the exception should be granted. The authority to make this determination cannot be delegated; and Division/Department Heads have the authority to impose more restrictive standards for electronically storing Personal Information in their area of responsibility.

Information Security Officer is responsible for recommending approval of an exception request based on a review of the documented circumstances and the proposed compensating controls for information security risks and technical reliability. The Information Security Officer role is held by the Director of Information Technology.

Data Stewards are responsible for complying with this Policy and any local requirements of their specific division or department to protect Personal Information.

Reason for Policy

LTC collects, stores, and uses Personal Information for its academic, patient care, community relations,

and business operations. LTC is committed to protecting Personal Information that is in its custody or control from unauthorized access, use, disclosure, disruption, or modification.

Historical Data, Cross References and Legal Review

Reviewed/Revised:
Legal Counsel Review and Approval:
Board Policy:

Definitions

Data Steward means LTC personnel who have Personal Information under their physical or logical control: for example, a faculty or staff member who places Personal Information on a Device; or a database administrator responsible for a campus wide or departmental database.
LTC personnel are not Data Stewards if they are:

1. Only users of a database (e.g., access or modify Personal Information via a web site or application screen and have no control over the ability to encrypt the database itself);
2. Do not store a local copy of Personal Information under their control; or
3. Do not have responsibility for the database itself.

Device means any computer or computing device, including, but not limited to, desktops, laptops, tablets (including iPads), smartphones, or removable media such as CDs, USB flash drives, or portable hard drives.

Division/Department Head means one of the following:

- President
- Vice President
- Chief Financial Officer
- Chief Human Resources Officer
- Director
- Dean

Personal Information means an individual's first name or first initial, and last name, *in combination with* any one or more of the following:

1. Social Security number;
2. Driver's license number or California identification card number;
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
4. Medical information, any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; and

Health insurance information, an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify an individual, or any information in an individual's application and claims history, including any appeals records.