POLICY TITLE:	Data Management and System Security	POLICY # 3.1	REVIEW DATES	
Topic Area:	INFORMATION MANAGEMENT		8/21/14	10/31/17
Applies to:	LRE Staff and Operations, Member CMHSP approved access users	ISSUED BY: Chief Executive Officer	9/1/2020	2/9/2024
Review Cycle:	Annual			
		APPROVED BY: Board of Directors		
Developed and Maintained by:	CEO and Designee			
Supersedes:	N/A	Effective Date: January 1, 2014	Revised Date: 02/09/24	

I. PURPOSE

To secure and protect electronic data used by the LRE staff and personnel and Member Community Mental Health Service Program (CMHSP) approved access users.

II. POLICY

Lakeshore Regional Entity (LRE) staff and personnel and approved CMHSP access users will protect and secure information that is electronically generated, received or transmitted by systems it controls or grants access to. All system users are bound by security, confidentiality, and computer usage policies entered into as condition of employment with LRE or as an approved access user. These will be reviewed and acknowledged by all users annually. Access to systems is made for the purpose of completing LRE-related business. Any violation will be cause for corrective action up to and including termination.

Standards and Guidelines

A. Access privileges to systems shall be authorized by the LRE Chief Information Officer (CIO) or designee within the LRE Information Technology (IT) Team. Access to systems shall be on a need-to-know basis for the purpose of accomplishing prescribed duties. The use of LRE systems for political or unlawful use is strictly prohibited. All users must abide by state and federal regulations. The user or the user's executive is responsible to communicate to the IT Team any privilege changes required to complete assigned duties that may result from changes in job duties, including hires, transfers, and terminations.
B. Non-employees may be granted access, considered on an individual basis upon completion of a non-disclosure, LRE Privacy training attestation (when applicable), and LRE CIO approval, or an administrator appointed by the CIO.
C. Passwords and time-out periods shall be utilized at all times. Passwords shall be exclusive to each user and not shared. Time out periods shall be implemented based on the role of the user and the type of information being accessed. Users shall always logout of or lock their workstations and devices when unattended to prevent access by others.

D. Data transmissions outside the secure LRE network that contain Protected Health Information (PHI), as defined by HIPAA or LRE Compliance, or other sensitive information must comply with current standards for encryption and security, as defined by LRE, and authorized by the CIO. Data accessions from outside the secure LRE network must comply with current standards for encryption and security, as defined by LRE.
E. System, device, application use, and file access may be monitored.
F. Email shall be considered not private, and generally not secure. It is intended for business purpose only. If confidential information or projected health information is transmitted via email it must be encrypted during transmission and while at rest. The use of email to transmit protected health information should be avoided whenever possible if another, more secure, information transfer method is available.
G. Access controls (permissions) to data, applications, and files will be maintained and monitored by the CIO or designee responsible for managing and maintaining system access. Access controls will be granted and revoked by the IT Team based on a user's job duties and changes in job role. The principle of "least privilege" will be applied to all systems containing PHI.

III. APPLICABILITY AND RESPONSIBILITY

The policy applies to LRE staff, Member CMHSPs, and other external users approved for access to LRE systems.

IV. MONITORING AND REVIEW

The CEO and designee, will review the policy on an annual basis.

V. DEFINITIONS

A. **HIPAA:** Health Insurance Portability and Accountability Act
B. **Encryption:** A method to protect data in motion and/or at rest.

VI. RELATED POLICIES AND PROCEDURES

A. LRE Information Management Policies and Procedures including procedure 3.1A
B. LRE Compliance Policies and Procedures
C. LRE Compliance Plan

VII. REFERENCES/LEGAL AUTHORITY

A. Balanced Budget Act 1997
B. HIPAA Act 1996
C. HITECH Act 2009
D. MDHHS Medicaid Specialty Supports and Services Contract

VIII. CHANGE LOG

Date of Change	Description of Change	Responsible Party
12/16/21	Added definitions	CEO and Designee
02/09/24	Language clarifications	CEO and Designee
