PROCEDURE # 3.1A		EFFECTIVE DATE	REVISED DATE
TITLE:	DATA MANAGEMENT AND SYSTEM SECURITY	January 1, 2014	April 20, 2026
ATTACHMENT TO POLICY #: 3.1 POLICY TITLE: DATA MANAGEMENT AND SYSTEM SECURITY CHAPTER: INFORMATION MANAGEMENT		REVIEW DATES 8/21/14, 10/31/17, 9/1/2020, 12/12/2021, 2/9/2024, 4/20/2026	

I. PURPOSE

To establish a procedure to secure and protect electronic data used by the Lakeshore Regional Entity (LRE) staff and personnel and Member Community Mental Health Service Program (CMHSP) approved access users.

II. PROCEDURES

A. Request for Access to LRE Systems

1. The individual requesting access will send a written request or submit a technical support ticket to the Chief Information Officer (CIO), or individual(s) designated by the CIO for granting system access, specifying the system needed and stating the reasons for need of access.
2. The CIO or designee will evaluate the request determining the need for access consistent with user role-based functions and tasks and appropriate non-disclosures and trainings. Requests for access to data that contains PHI will require documentation of LRE Privacy training and attestation prior to approval.
3. The CIO or designee will refer the applicant to the most appropriate (LRE or CMHSP) training resources to complete the necessary trainings and documentation. All supporting documentation will be maintained on the LRE SharePoint site.
4. The CIO or designee will approve system access upon confirmation of completion of required training and attestations. The CIO or designee may grant access and admittance for LRE ROAT group members at the request of the CMHSP CEO without requiring a signed access request form.
5. Information systems management will maintain an updated log of individuals that have access to systems.

B. Cyber Security Incident Reporting

1. All workforce members must immediately notify the IT department upon discovering or suspecting a cybersecurity incident. LRE workforce members should report issues quickly by emailing the IT Helpdesk and calling the IT Helpdesk Lead phone number.

2. Anyone who suspects that they may have inadvertently shared their password with a bad actor should change it immediately at: My Sign-Ins | Recent Activity | Microsoft.com

3. Individuals must not attempt to investigate, remediate, or resolve suspected cyber incidents on their own unless explicitly directed to do so by a member of the IT team.

4. Failure to promptly report a cybersecurity incident may increase risk to the organization and may result in corrective action or other sanction.

5. If you are not sure whether you are facing a cybersecurity incident or not, remember, **when in doubt, report the incident.**

   When reporting incidents, include the following information if possible:
   - Date and time the incident was noticed
   - Description of what occurred or what was observed
   - Screenshots of alerts, notifications, or suspicious activity
   - Affected system(s), device(s), or account(s)
   - Any actions already taken (if any)

   Prohibited actions: To preserve evidence and support proper investigation, workforce members must **not**:
   - Delete files, emails, or logs related to the incident
   - Shut down or disconnect systems or eliminate network connection of an infected device (unless instructed to do so by IT).
   - Attempt to "fix" or mitigate the issue themselves, except changing the account password and clicking "Sign out everywhere".
   - Share incident details outside authorized reporting channels

   IT responsibilities: Upon notification, IT will:
   - Assess severity and potential impact
   - Initiate containment, investigation, and remediation activities
   - Determine whether the incident meets breach or regulatory reporting thresholds
   - Coordinate with leadership, Compliance, Legal, Privacy, and external partners as required

III. APPLICABILITY AND RESPONSIBILITY

The procedure applies to LRE staff and contracted workforce members, Member CMHSPs, and other external users approved for access to LRE systems.

IV. MONITORING AND REVIEW

The Chief Information Officer, in conjunction with the Chief Executive Officer, will review the procedure on an annual basis.

V. DEFINITIONS

Cybersecurity Incident: A cybersecurity incident includes but is not limited to:

- Suspected or confirmed malware, ransomware, or virus infections
- Entering credentials because of Phishing emails, suspicious links, or unexpected attachments
- Unauthorized access to systems, accounts, or data
- Loss or theft of devices containing organizational data
- Accidental or unauthorized disclosure of sensitive information (including PHI, PII, or financial data)
- System behavior that is unusual, degraded, or unexplained
- Failed security controls, alerts, or warnings indicating possible compromise

VI. RELATED POLICIES AND PROCEDURES

A. LRE Information Management Policies and Procedures
B. LRE Compliance Policies and Procedures
C. LRE Compliance Plan
D. LRE Cybersecurity Incident Response Plan

VII. REFERENCE/LEGAL AUTHORITY

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

VIII. CHANGE LOG

Date of Change	Description of Change	Responsible Party
12/16/21		CIO
02/09/24	Language updates	CIO
04/20/26	Added section: Cybersecurity Incident Reporting (and associated definitions). Minor language updates	CIO