



# **RISK MANAGEMENT PLAN 2024**



**Community**

MENTAL HEALTH

CLINTON • EATON • INGHAM

*Together we can.*

March 2024

# **Table of Contents**

<b>01</b>	<b>Overview</b>
<b>01</b>	<b>Areas of Risk/Exposure</b>
<b>01</b>	<b>General Strategies Used to Address Risk</b>
<b>02</b>	<b>Risk Assessment and Management Control Tool</b>
<b>03</b>	<b>Risk Management Map</b>
<b>03</b>	<b>    General Liability</b>
<b>06</b>	<b>    Professional Liability</b>
<b>06</b>	<b>    Liability to Staff/Employees</b>
<b>09</b>	<b>    Liability to Consumers</b>
<b>12</b>	<b>    Contractual Liability</b>
<b>12</b>	<b>    Business Loss/Interruption</b>
<b>13</b>	<b>    Loss of Reputation</b>
<b>16</b>	<b>Planned Actions to Mitigate Risk</b>
<b>16</b>	<b>Related Policies and Procedures</b>

## Overview:

Risk management – involves engaging in activities that deal with uncertainty and potentially harmful future events.

To accomplish the goal of effectively managing risks, a Risk Management and Controls System tool has been developed to assist CMHA-CEI in identifying and analyzing loss exposure and safety hazards, control mechanisms, responsibility and scheduling of reporting and monitoring the results produced or achievement of changes. The areas of exposure/risk are tracked through all the sites of the organization.

The purpose of this Risk Management Plan is to:

- Identify and minimize risk to CMHA-CEI, the individuals served by the agency, and the agency's staff and volunteers
- Address risk and increase awareness about identifying risk and how to minimize it
- Assist in preventing harmful events
- Protect the consumers of the agency
- Protect the agency's reputation and assets
- Ensure the continuity of service provided by the agency
- Utilize a practical and common sense approach that that considers the need of the individuals being served first and foremost

This Risk Management Plan co-exists with the agency's risk management policies and procedures.

## Areas of Risk/Exposure:

CMHA-CEI faces many risks in the course of its daily operations. The majority fall in to one of the following categories:

- **General liability**
- **Professional liability**
- **Liability to Employees**
- **Liability to Consumers**
- **Contractual Liability**
- **Business Loss / Interruption**
- **Loss of Reputation**

## General Strategies Used to Address Risk:

CMHA-CEI works to minimize undesirably high risks through the use of policies, procedures, trainings, equipment and tools, and supervision. In addition, the following techniques are utilized to manage risk.

- **Avoidance** –discontinuing an activity, refusing to offer a service, and/or declining to undertake business ventures that are unsafe and unsuitable for staff and/or for consumers served by the organization for the purpose of avoiding undesirably high risks
- **Modification** (Loss Prevention and Loss Reduction) – implementing activities to reduce the level of risk (e.g., policies and procedures)
- **Retention** – accepting all or part of the risk and preparing for potential consequences by accepting deductible costs or self-insuring

## Risk Assessment & Management Control Tool:

CMHA-CEI's **goal** is to promote quality services to our consumers and their families and manage risk effectively.

Staff members are well trained for the job duties and responsibilities in their daily functions. This assessment & management control tool assesses the level of organizational exposure to risks, incorporates systems of checks and balances that clearly define accountability and monitor critical performance variables, and identifies the need additional controls. Control systems are designed to minimize risks and prevent and detect illegal or unethical activity, and/or fraud, waste and abuse. Access to critical information is on a need to know basis.

Exposure	Frequency	Potential Severity of Impact	Control Mechanism	Risk Reduction	Responsibility	Review Date	Action Steps
----------	-----------	------------------------------	-------------------	----------------	----------------	-------------	--------------

- **Exposure** – area of potential risk
- **Frequency** (Low-Moderate-High) – likelihood of risk occurrence
- **Potential Severity of Impact** (Low-Moderate-High) – level of effect
- **Control Mechanism** – Policies, procedures
- **Risk Reduction Effectiveness** (Low-Moderate-High) – how effective is the control mechanism(s) in reducing risk for an exposure
- **Responsibility** – Agency personnel tasked with overseeing area of risk
- **Review Date** – The frequency with which risk and associated control mechanisms are reviewed
- **Action Steps** – strategies and methods used to manage the risk



# Risk Management Map

## General Liability

General liability refers to the amount of loss payable to others outside the organization for injury and/or damage arising from agency operations. It applies to personal injury, bodily injury and damage to a third party resulting from the negligence of the program operations or the staff.

Exposure	Frequency	Potential Severity of Impact	Control Mechanism	Risk Reduction	Responsibility	Review Date	Action Steps
Clinical staff while providing services in the buildings	Low	Mod	Liability insurance; personal safety training, Workplace Violence Prevention Training (which includes Situational Awareness, Victim Avoidance, Active Shooter, and an overview of the Workplace Violence Prevention Program), and on-call training	Mod	Chief Human Resource Officer; Environmental Safety and Compliance Officer	Annually	Provide training and monitor staff compliance with training requirements.
Consumers coming into the buildings for treatment	Mod	High	Liability insurance and safety drills and training, monthly self-inspections for hazards	High	Chief Human Resource Officer; Environmental Safety and Compliance Officer	Annually at renewal and monthly safety checks	Policies and procedures are followed and regularly reviewed by staff, staff receive orientation and training in a number of areas including safety and prevention, (e.g., , first aid, blood borne pathogens, etc.), injuries, incidents and accidents are reported and reviewed by HR to identify any trends

Mental health professionals working in the community	Low	High	Worker's compensation Insurance, Liability insurance; personal safety training, Workplace Violence Prevention Training (which includes Situational Awareness, Victim Avoidance, Active Shooter, and an overview of the Workplace Violence Prevention Program) and on-call training	Mod	Chief Human Resource Officer; Environmental Safety and Compliance Officer	Annually	Policies and procedures are followed and regularly reviewed by staff, staff receive orientation and training in a number of areas including safety and prevention (e.g., , first aid, blood borne pathogens, etc.), injuries and accidents are reported and reviewed by HR to identify any trends. Follow up of any incidents reported also occurs by HR, facilities, or supervisor to review the incident with the staff and how to prevent in the future. Staff have cell phones available to call for help, if necessary. Implementing an emergency alert system to alert staff of incidents including tornado, active shooter and shelter in place. Workplace violence training for all staff was conducted in 2019.
Misuse of stored or handled medications	Mod	High	Policies and procedure on medication management: storage, administration, inventory, disposal	High	Corporate Compliance Officer; Director of Quality, Customer Service and Recipient Rights	Annually	Contract Pharmacy conducts site visits to group homes and any concerns are addressed within the Medication and Pharmacy Workgroup. QI reviews any reported medication incidents and follows up and provides additional training as needed.

Injury of an unauthorized individual on agency equipment	Mod	Mod	Security cameras with review of tapes as concerns arise, signed waivers, liability insurance, member rules	High	Environmental Safety and Compliance Officer	Annually	Security systems set up to ensure only authorized staff have access to designated agency areas via ID badge.
Animals in the building (i.e., consumer mobile and emotional support animals)	Low	High	Liability insurance, procedure on animals in the buildings	High	Environmental Safety and Compliance Officer	Annually	Developed Animals in CMHA-CEI Buildings Procedure 1.7.02A to address animals in the building
Phishing Scams – emailing Finance and requesting a payroll direct deposit bank account change. Email or texts to staff requesting the purchase of gift cards or financial transfers of payments.	Low	Mod	Finance Department has a verification process in place to obtain verbal confirmation of any changes for financial transactions. IS Department security flags emails from external accounts and monitors that the flagging system is active	Mod	Chief Financial Officer  HIPAA Security Officer	Annually	Finance Department updates a list of known Provider Contacts and maintains a list of approved individuals that can update payment information. Staff reminders are sent about cyber safety and efforts to increase staff awareness about external links or emails.

### Professional Liability

The highest risk of exposure is in the area of service provision. CMHA-CEI is responsible for carrying professional liability insurance for all its staff members.

Exposure	Frequency	Potential Severity of Impact	Control Mechanism	Risk Reduction	Responsibility	Review Date	Action Steps
Clinical staff and Medical staff	Low	High	Licensure and trainings, Professional Liability Insurance, Regular supervision of staff, annual evaluations to assess competence & scope of practice, processes for conducting background checks using other States' records databases for new out-of-state hires	High	CHRO	Annually	HR credentials staff at hire and every 2 years. OIG reports are run monthly to check for staff exclusions.
Threat of lawsuit due to allegations of malpractice	Mod	High	Professional Liability Insurance, on-going staff training and supervision. Reporting potential incidents to management and insurance carrier, thorough documentation of potential incidents and steps taken.	Mod	CEO	Insurance policy reviewed annually, ongoing monitoring on case-by-case basis	The malpractice insurance provider requires that CMHA-CEI notifies when there is a possibility of a malpractice lawsuit. Consultation with the insurance provider may result in additional action steps.

### Liability to Staff/Employees

Exposure	Frequency	Potential Severity of Impact	Control Mechanism	Risk Reduction	Responsibility	Review Date	Action Steps
----------	-----------	------------------------------	-------------------	----------------	----------------	-------------	--------------

Staff may be exposed to various occupational accidents including falling, tripping, straining, etc.	Mod	Mod	Injury reporting and tracking to determine trends and methods for preventing injures. On-going staff training on safety issues and practices to prevent injury. Facility & grounds physical improvements and repairs Pre-employment drug testing	High	Chief Human Resource Officer; Environmental Safety and Compliance Officer	Each Incident and by Safety Committee	Each month the Environmental Safety and Compliance Officer provides information regarding a different safety topic to all agency staff. The theme of the safety topic is relevant to seasonal differences or may be impacted by other relevant topics. Additional safety documents are provided to staff that provide information on how to maintain safety.
General security building, vehicle, transportation, and health and safety for staff.	Low	Mod	Regular Safety Committee meetings with department representatives and safety officers.	Mod	Environmental Safety and Compliance Officer	Annually	Review and update Safety Committee structure and process to ensure effectiveness.
People entering CMHA-CEI buildings that may represent a threat to staff and/or consumers	Low	High	Staff Training in Crisis Prevention and workplace violence. Emergency Procedures and phone alerts. Badge Access to most suites. Updated building watchlist, procedures and monitoring process.	High	Environmental Safety and Compliance Officer	Each Incident and by Safety Committee	A watchlist is connected to the front desk sign-in process, which flags persons who have been deemed persons of concern through investigations. Watchlist procedure and monitoring process have been updated. Procedures and training front desk staff on front lobby de-escalation were developed.
When clinicians are providing services in the community	High	High	Personal Safety Training for Staff. On-call available.	Mod	Chief Human Resources Officer; Environmental Safety and Compliance Officer;	Annually/On going	Work in tandem with Chief HR Officer and Training Coordinator to ensure that staff whose training category requires Personal Safety Training receive the required Training. Also HR and safety officer reviews any incident reports involving harm to employees while providing services in the community to identify any trends.

Exposure to hazardous bodily fluids	Low	Mod	Training on Blood Borne Pathogens. Procedures on Exposure	High	Environmental Safety and Compliance Officer; Corporate Compliance Officer	Orientation and Annually. Incidents reviewed monthly during Critical Incident Committee and Safety Committee for staff	Provide BBP Clean up Kits and utilize universal precautions when interacting with bodily fluids Work with Safety Committee (for staff exposures) and QCSRR staff (for consumer exposure) to ensure that the appropriate Incident Reports are reviewed and identify any trends that may be present to then develop plans to mitigate future risk. Have an Exposure Control Plan that was developed by Property and Facilities.
Exposure to hazardous chemicals for cleaning or maintenance	Low	Mod	Material Safety Data Sheets kept at each work location	High	Environmental Safety and Compliance Officer	Ongoing	Limit employee interaction and exposure to chemicals. Assign "commercial" cleaning activities to staff that have been trained on the chemicals which they will be using. Have an Exposure Control Plan that was developed by Property and Facilities.
Illness/communicable disease	Low	High	Staff are encouraged to stay home when ill, Staff are trained in preventing communicable disease, Agency is disinfected by cleaning crew on regular basis, Infection control policies, active Virus Task Force to review any incidents of communicable diseases	Mod	Environmental Safety and Compliance Officer	Ongoing	At start of COVID Pandemic developed a Virus Task Force to develop agency protocols around COVID and communicable diseases. Have email box for staff to send questions. Virus Task Force meets regularly to review federal, state, and local mandates, review current protocols, develop communication tools to staff, monitor supplies, etc. Also developed a recovery plan when having to pause operations due to a Pandemic to outline steps to resume normal operations.

Staff turnover	Low	Mod	Wage and benefit package, Staff retention plan, HR policies designed to ensure a safe workplace, Employee recognition, Grievance procedure, Orientation and training	Mod	Chief Human Resource Officer	Ongoing	Agency has developed Recruitment and Retention Plan including wage increases, retention payments, expanded student debt relief and wage and compensation studies for positions. Also implemented a Media Campaign for hiring. Continue Manager trainings and manager support.
----------------	-----	-----	---	-----	------------------------------	---------	---

**Liability to Consumers**

Exposure	Frequency	Potential Severity of Impact	Control Mechanism	Risk Reduction	Responsibility	Review Date	Action Steps
Administrative Litigation on abuse and neglect	Low	High	Code of Ethics and policy on reported suspected abuse and neglect	High	Director of Quality, Customer Service and Recipient Rights	Ongoing	Provide recipient rights training to new employees within 30 days of hire and annually; maintain Rights Office according to State requirements.
Exploitation of consumers with cognitive disabilities	Low	High	Code of Ethics. Progressive discipline system. Consumer concerns and complaint procedure	High	Director of Quality, Customer Service and Recipient Rights	Ongoing	Provide recipient rights training to new employees within 30 days of hire and annually; maintain Rights Office according to State requirements.

<p>False billing of consumer services</p>	<p>Low</p>	<p>High</p>	<p>Corporate compliance procedures, financial policies and procedures, concerns and compliments system, Code of Ethics, Admission and billing procedures. Implementation of functional EHR incorporating validations to protect against errors and inaccurate billing</p>	<p>High</p>	<p>Chief Financial Officer; Corporate Compliance Officer</p>	<p>Ongoing</p>	<p>Complete Medicaid Event Verification process internally, and through MSHN bi-annually. Pursue recoupment as necessary and report to OIG as required.</p>
<p>Computer Network System – information loss/shut down due to virus, hackers, spam, etc.</p>	<p>Low</p>	<p>High</p>	<p>Multiple vendor heuristic and definition based anti-virus, intrusion protection, and anti-malware scanning at the endpoint, virtual machine, email system, and firewall levels. Daily backups of network data with procedural accommodation for data verification and offsite storage. Use of contracted vendors for automated scanning of externally facing systems against known vulnerabilities as well as scheduled non-automated penetration testing.</p>	<p>Mod</p>	<p>HIPAA Security Officer</p>	<p>Logs for intrusion prevention, anti-virus, &amp; anti-malware systems are reviewed daily by IS staff. Automated scans are run and reviewed weekly. Non automated penetration tests are scheduled bi-yearly.</p>	<p>All vendor contracts for anti-virus, anti-malware, and intrusion prevention are reviewed the year they expire against the current landscape of available vendors for innovations in the field that could better serve our organization.</p>

<p>Information Management – unauthorized disclosure of protected health information</p>	<p>Low</p>	<p>High</p>	<p>Security and policies and procedures. Annual Security Analysis. Processes for handling information on agency equipment and software (i.e., copiers, scanners, fax machines, use of email, texting, etc.) Secure\encrypted email services provided to employees for transmission of EPHI to external contacts. External vendors contracted for secure destruction of expired or failed magnetic media.</p>	<p>Mod</p>	<p>HIPAA Security Officer; Corporate Compliance Officer</p>	<p>Annually</p>	<p>Monitor office spaces and ensure wall/barrier to separate areas for purposes of security &amp; privacy Compliance reporting processes and reports developed if needed to monitor access to records.</p>
<p>Injury of consumer in accident when providing transportation</p>	<p>Mod</p>	<p>High</p>	<p>Driver's license checks at hire, and review annually and as incidents are reported. Pre-employment drug testing.</p>	<p>Low</p>	<p>Chief Human Resource Officer; Environmental Safety and Compliance Officer</p>	<p>Annually</p>	<p>Resources are available to staff on the intranet to assist with planning commutes in regards to the current and forecasted weather, as well as current traffic conditions. GPS devices are installed on the vehicle, allowing the admin to observe any risky vehicular actions taken by a driver (hard braking, speeding, etc.), discouraging reckless driving. Emails out to staff when hazardous weather conditions so they can be prepared if needing to provide transportation.</p>

### Contractual Liability

Contractual liabilities can arise out of leases, rental agreements, special service agreements, joint use agreements, cooperative ventures, and construction contracts.

Exposure	Frequency	Potential Severity of Impact	Control Mechanism	Risk Reduction	Responsibility	Review Date	Action Steps
Other Contracted Services	High	Mod	Carries own malpractice insurance, liability, & auto insurance	High	Chief Financial Officer	Annually	Providers are credentialed initially and every 2 years. Many provider types also receive an annual site visit. Developed a monthly contract and compliance committee meeting to review any provider concerns.

### Business Loss/Interruption

Loss or reductions business has direct impact on CMHA-CEI financial status. Business interruption in any site could cause significant loss to the agency.

Exposure	Frequency	Potential Severity of Impact	Control Mechanism	Risk Reduction	Responsibility	Review Date	Action Steps
Loss of Medicaid contract	Low	High	Regionalization	High	Chief Executive Officer, Chief Financial Officer, Director of Quality, Customer Service, Recipient Rights	Ongoing	Annual Financial audit is completed through external agency. Annual Audit through PIHP is conducted. Quality Improvement team performs regular reviews to ensure compliance with Medicaid contract. Agency completes MDHHS and PHIP reporting requirements.

Extended power outage would affect ongoing business operations of billing for services and thus cash flow for payment of employees and expenses	Low	Mod	Offsite back up of computer systems with ability to access from home or other location. Update policies and procedures related to backup and testing. Installation of a generator at main office	Mod	HIPAA Security Officer, Environmental Safety and Compliance Officer	Annually	CMHA-CEI updated the Emergency Closing of CMHA-CEI Programs Procedure which outlines the process and circumstances for closing dur to environmental emergencies; snow/ice conditions, tornadoes/severe weather, utility outages, and public health emergencies.
Cyber Security – Any cyber breach brings significant financial risks and harm to the reputation of the agency, as well as potential operation interruption.	Mod	High	Cyber Security related policies and procedures guide defense against cyber threats. The IS team has a position dedicated to security efforts and monitoring system effectiveness. Regular staff reminders are sent about cyber safety and efforts to increase staff awareness about external links or emails.	Mod	Chief Executive Officer, Chief Information Officer, Chief Financial Officer	Annually	Review Cyber Security related policies and procedures for accuracy and effectiveness. Review updated cyber security regulations and software security measures.

**Loss of Reputation**

Exposure	Frequency	Potential Severity of Impact	Control Mechanism	Risk Reduction	Responsibility	Review Date	Action Steps
----------	-----------	------------------------------	-------------------	----------------	----------------	-------------	--------------

Loss of accreditation	Low	Low	Continuous review of CARF standards	High	Director of Quality, Customer Service, Recipient Rights	Ongoing	Review progress toward CARF plan of correction at Quality and Compliance Committee Meetings, and monitor by Quality, Customer Service and Recipient Rights department.
HIPAA violation and resultant investigation by Office of Civil Rights	Mod	High	HIPAA policies, and annual & periodic trainings during the year	High	Corporate Compliance Officer	Ongoing	HIPAA Privacy Violation and Mitigation. Working to codify the process for routinizing the Auditing Compliance Reporting Processes.
Administrative litigation on abuse or neglect	Low	High	Code of Ethics	Mod	Director of Quality, Customer Service, Recipient Rights	Ongoing	All staff receive annual training on Recipient Rights. Regularly review updated guidance with legal and Directors.
Embezzlement or misuse of organization monies	Loe	High	Strong Internal Control Policies with segregation of duties. Code of Ethics	High	Chief Executive Officer, Chief Financial Officer	Ongoing, annual audit	The CMHA-CEI Finance Department participates in an external audit annually.

Board of Directors – Governance - Criminal activity, fraud, theft, legal requirements, liability, conflict of interest	Low	Mod	Liability insurance, Governance policies and procedures, Separate of duties/functions, Board member orientation, Committee oversight	High	Chief Executive Officer	Ongoing	A set of bylaws are enforced for Board of Directors. Board members receive training and updates from the CEO.
Administrative litigation resulting from disclosure or discoverability of documents that are beyond document retention requirements (This includes both paper as well as electronic documents and emails)	Mod	High	Strong policies and procedures on document retention and destruction. Active practices for the regular destruction of documents according to CMHA-CEI and State policies. Storage of historical electronic documents on updated application allows for auditing & disposal.	High	HIPAA Security Officer; Corporate Compliance Officer	Ongoing	Develop record retention processes with Electronic Health Record vendor.
Media: Inappropriate contact with the media, and misuse of social media	Mod	High	Policies on contact with the media, and on expectations on use of social media, agency procedures on staffs' personal social media use & representation of agency/work topics. Restricted and designated access to use of agency social media sites.	Mod	Chief Executive Officer	Ongoing	Policies and procedures on use of social media are reviewed annually. Human Resources Department and supervisor will address any concerns as they arise. Have a Public Relations position that support programs on social media posts for work related purposes

## Planned Actions to Mitigate Risk

Action	Responsibility	Risk Category
Follow process for destruction of documents after retention period	Corporate Compliance Officer; HIPAA Security Officer	Loss of Reputation
Continue Recruitment and Retention Plan and review applicable data to see impact	Chief Human Resource Officer, Chief Executive Officer.	Liability to staff/employees
Review and update Safety Committee structure and process to ensure effectiveness	Property and Facilities Manager	Liability to staff/employees
Codify the process for routinizing the Auditing Compliance Reporting Processes.	Corporate Compliance Officer	Loss of Reputation
Update credentialing of staff and contracted agencies to align with updates state guidance	Chief Human Resource Officer, Chief Financial Officer.	Professional Liability
Review liability insurance packages to ensure proper coverage	Property and Facilities Manager, Chief Financial Officer, and Chief Executive Officer	General Liability
Review cyber security related policies and procedures for accuracy and effectiveness. Review updated cyber security regulations and software security measures.	Chief Executive Officer, Chief Information Officer, Chief Financial Officer	Business Loss/Interruption

### Related Policies and Procedures:

- Risk Management Policy 1.1.13
- Sentinel Event Policy 1.1.14
- Sentinel Event Procedure 1.1.14
- Compliance Policy 1.1.04
- Breach Notification Protected Health Information Procedure 1.1.17
- Information Systems Security Procedure 1.5.01D
- Email Use and Responsibility Procedure 1.5.01E

### Review Period:

The Risk Management Plan is reviewed annually per CARF requirements.