Chapter Title	Chapter #		Subject #
Fiscal	F		282.12

Subject Title **Security Management**	Adopted 3/15/05	Last Revised 4/20/21	Reviewed 3/15/05; 4/23/10; 2/24/14; 5/12/15; 9/15/15; 3/17/17; 3/18/19; 3/18/20; 5/12/20; 4/20/21; 4/21/22

PROCEDURE

The purpose of security management is to prevent, detect, contain, and correct security breaches through risk analysis, appropriate configurations, and systems modifications.

Application

This procedure shall apply to The Right Door for Hope, Recovery and Wellness.

1.0   Security Incident

Security Incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations.

In the event if a security incident, the CFO shall immediately inform the CEO. It is the discretion of the CEO to proceed as needed with investigations, actions, and disciplinary measures. In addition, the CEO or designee shall report the incident to the Mid State Health Network.

All security incidents will be referred to the Compliance Officer.   After documented, each incident will be investigated.   If corrective action must occur, the corrective action and date it is completed will be documented.

2.0   Internal Audit

Internal audits will be performed periodically in an attempt to minimize security incidents. Audits may include, but are not limited to, facilities tours, review of log files, systems review. Results of findings will be documented and kept.

Chapter Title	Chapter #		Subject #
Fiscal	F		282.12

Subject Title	Adopted	Last Revised	Reviewed
Security Management	3/15/05	4/20/21	3/15/05; 4/23/10; 2/24/14; 5/12/15; 9/15/15; 3/17/17; 3/18/19; 3/18/20; 5/12/20; 4/20/21; 4/21/22

IS Department Audit practices must include the following components:

- Periodic review of EHR accessibility for appropriate use of system. This information is prepared by IS and performed under the authority of the agency Compliance Officer. The compliance officer received the results of the supervisor reviews and performs any necessary follow up. IN addition to supervisors reviewing staff access, the Compliance Committee reviews the agency "break-the-glass" system report for appropriate use.
- Periodic review (minimum weekly) of Firewall executive reports (generated daily, weekly, and monthly) and port scan notifications for potential issues.
- Ongoing monitoring of backup processes for successful completion
- Ongoing monitoring of device patching and versioning with appropriate prioritized follow up as determined necessary.
- Weekly review of system component log files for unusual/inconsistent activity.

3.0   Minimum Necessary

The idea of "minimum necessary" will be employed at The Right Door for Hope, Recovery and Wellness. This entails only granting access permissions and authorization to data that is required to perform one's job duties and nothing more.

4.0   Access Authentication

Prior to establishing (or modifying) access to resources containing protect health information (PHI), a needs assessment will be performed to check

Chapter Title	Chapter #		Subject #
Fiscal	F		282.12
Subject Title **Security Management**	Adopted 3/15/05	Last Revised 4/20/21	Reviewed 3/15/05; 4/23/10; 2/24/14; 5/12/15; 9/15/15; 3/17/17; 3/18/19; 3/18/20; 5/12/20; 4/20/21; 4/21/22

whether or not this change in access meets the minimum necessary criteria. The same process will be applied when changes are requested to existing permissions.

5.0   Risk Analysis
A risk analysis will be performed prior to making changes to systems configurations or loading programs. The benefits of the change will be compared with the negatives and a determination will be made by the CFO whether or not to make the change.

6.0   Risk Management

Risk shall be managed by minimizing the chances of security incidents. This will be accomplished by ensuring proper systems configurations, employing minimum necessary rules to all aspects of The Right Door for Hope, Recovery and Wellness network, and by providing training for all users on important security related issues.

7.0   Sanctions

Sanctions for violating security policies and procedures shall be employed evenly and fairly to all members of the organization. Exact disciplinary actions will be handled on a case-by-case basis by the CEO.

8.0   Business Associate Agreements

Business Associate Agreements will be held between The Right Door for Hope, Recovery and Wellness and all necessary parties as outlined in the HIPAA Security Regulations.

The Right Door for Hope, Recovery and Wellness

Chapter Title	Chapter #		Subject #
Fiscal	F		282.12
Subject Title **Security Management**	Adopted 3/15/05	Last Revised 4/20/21	Reviewed 3/15/05; 4/23/10; 2/24/14; 5/12/15; 9/15/15; 3/17/17; 3/18/19; 3/18/20; 5/12/20; 4/20/21; 4/21/22

This Policy encompasses HIPAA Security Regulations, "Security Incident Procedures", section 164.308(a)(6), "Evaluation", section 164.308(a)(8), "Information Access Management", section 164.308(a)(4), "Security Management Process", section 164.308(a)(1), and "Business Associate Contracts and Other Arrangement", section 164.308(b)(1).

Kerry Possehn, Chief Executive Officer	Date		