Chapter Title	Chapter #		Subject #
Fiscal	F		282.10
Subject Title **Contingency Plan/Systems Data Backup**	Adopted 3/15/05	Last Revised 5/12/20	Reviewed 3/15/05; 4/30/08; 4/23/10; 8/25/15; 3/15/17; 3/18/19; 5/12/20; 4/6/21; 4/21/22

PROCEDURE

The Right Door for Hope, Recovery and Wellness resources are available for use at all times. This encompasses ensuring maximum availability of MIS resources.

Application

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

1.0 Resource Outages

In the event of a resource outage, the end user community will be notified at least twenty-four hours in advance of the outage (if planned), or within twenty-four hours of the outage (if unplanned).

2.0 Data Criticality

Certain applications are considered mission critical if in the event of the loss of the resource, consumer treatment would be disrupted. The order of critical applications is as follows:

a. Electronic Health Record EMR
b. Email
c. Visual Account Mate Accounts Payable System
d. File and Print Services
e. Intranet

3.0 Disaster Recovery

In the event of a catastrophic systems failure (system resource loss), the following actions shall be taken by MIS department staff:

a. Assess the situation to determine the extent of the problem. Determinations of resource needs (new or used) can be made.
b. Implement replacement functionality as soon as possible.
c. Restore required data as applicable.

4.0 File server and Email Server Backup

The Right Door for Hope, Recovery and Wellness file servers and email servers are backed up following the MIS Department backup process. Backups are

Chapter Title	Chapter #		Subject #
Fiscal	F		282.10
Subject Title **Contingency Plan/Systems Data Backup**	Adopted 3/15/05	Last Revised 5/12/20	Reviewed 3/15/05; 4/30/08; 4/23/10; 8/25/15; 3/15/17; 3/18/19; 5/12/20; 4/6/21; 4/21/22

stored on both local and offsite storage devices. Files and email stored in the organizational Office 365 account are governed by the Office 365 data retention policy. A backup is also run prior to the application of any software or operating system patches.

5.0 Firewall Configuration File Backup

The firewall configuration files are backed up to a network share on a daily basis. Additionally, before making any changes to the configuration of the firewall, a backup of the current configuration is completed. Also, a backup is completed prior to the installation of any software or firmware updates.

6.0 Backup Rotation

Backup copies of organizations servers will follow the MIS Backup process outline. Daily copies will be maintained up to 14 days a appropriate. Monthly copies shall be retained for up to 12 months.

7.0 Emergency Mode Operations

Limited operational capacity will be available in the event of an emergency (examples include fire, power outage, etc.). If computer resources are unavailable, a paper mechanism will be used until operations can be restored.

8.0 Testing and Revisions

Testing data backups shall occur at least once per quarter. This will encompass ensuring that data on backup drives is valid and by performing a sample restoration.

Revisions to these procedures will be made as needed to accommodate needs.

This policy encompasses HIPAA Security Regulations, "Contingency Plan", section 164.308(a)(7).

Kerry Possehn, Chief Executive Officer	Date		