

The Right Door for Hope, Recovery and Wellness

Chapter Title Fiscal	Chapter # F		Subject # 282.10
Subject Title <b>Contingency Plan/Systems Data Backup</b>	Adopted 3/15/05	Last Revised 4/30/08; 8/25/15; 3/15/17	Reviewed 3/15/05; 4/30/08; 4/23/10; 8/25/15; 3/15/17

**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**

Server 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. Visual Account Mate Accounts Payable System
- c. File and Print Services
- d. Email
- e. Intranet

**3.0 Disaster Recovery**

In the event of a catastrophic systems failure (server resource loss), the following actions shall be taken:

- 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.

**4.0 File server and Email Server Backup**

All The Right Door for Hope, Recovery and Wellness file servers and email servers are backed up every night from the central backup. The backup software package we run is Arcserve UDP. Monday through Thursday, a differential backup is done; all files that have been modified since the last full backup are

## The Right Door for Hope, Recovery and Wellness

Chapter Title  Fiscal	Chapter #  F		Subject #  282.10
Subject Title <b>Contingency Plan/Systems Data Backup</b>	Adopted 3/15/05	Last Revised 4/30/08; 8/25/15; 3/15/17	Reviewed 3/15/05; 4/30/08; 4/23/10; 8/25/15; 3/15/17

written. A full backup of all file and email servers is completed every Friday and the tape stored in a secure location off site. A backup is also run prior to the application of any software or operating system patches; this backup is permanently archived off site. Additionally, one backup per quarter is archived for a full year, with the 4<sup>th</sup> quarter backup archived permanently each year. A repair disk is also created once per quarter for each Windows 2003/Windows 2008 server, as well as a backup of all registry keys related to shares. This allows the emergency repair process to be run, and minimizes the time required to recreate shares if a rebuild of the server is required. These disks are permanently archived in a secure off site location.

Additionally, Arcserve UDP will be used to create IDR cd's of all server at least quarterly, or whenever hardware and/or major software changes, or configuration changes are completed. These cd's will be stored at the offsite emergency disaster recovery location.

### **5.0 Firewall Configuration File Backup**

The firewall configuration files are backed up to a network share on a quarterly 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 Tape Rotation**

One of the most commonly used tape rotation schemes is called "Grandfather-Father-Son". We use a variation of this scheme. Two sets of daily backup tapes are stored on site, and two sets of Friday drives are stored in a secure location off site. A third drive for quarterly backups is also kept in a secure off site location.

The first hard drives, "Son," represent your daily backups. Five tapes are assigned as daily backups and labeled "Monday Week 1" through "Thursday Week 1," and "Monday Week 2" through "Thursday Week 2", these tapes will be used to perform daily backups and can be reused biweekly on the day that they are labeled.

A hard drive, called "Father," is used to perform Friday full backups. This media set should be labeled "Friday Even" and "Friday Odd" and can be reused biweekly on the day matching its label.

The Right Door for Hope, Recovery and Wellness

Chapter Title Fiscal	Chapter # F		Subject # 282.10
Subject Title <b>Contingency Plan/Systems Data Backup</b>	Adopted 3/15/05	Last Revised 4/30/08; 8/25/15; 3/15/17	Reviewed 3/15/05; 4/30/08; 4/23/10; 8/25/15; 3/15/17

The final hard drive, called “Grandfather,” is used to perform full backups on the last business day of each quarter.

This rotation scheme will back up on a daily, weekly, and quarterly basis. The 4<sup>th</sup> quarter backup tape is pulled from the rotation, relabeled as a yearly backup, and permanently archived in a secure location off site.

**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 tapes 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).*

Robert S. Lathers, Chief Executive Officer	Date		